Aalto-yliopisto
Kauppakorkeakoulu

"YRITYSJOHDON VASTUU/TILIVELVOLLISUUS YRITYKSEN KYBERTURVAKYSY-MYKSISSÄ"

Kuvaileva/tutkiva tapaustutkimus kyberturva-asioiden vastuunjaosta

Maisterin tutkielma

Jere Rignell

Aalto-yliopiston kauppakorkeakoulu

Laskentatoimi

Syksy 2019

Aalto University
School of Business

Aalto University, PL 11000, 00076 AALTO
www.aalto.fi
Abstract of master's thesis

Author Jere Rignell

Title of thesis Management responsibility/accountability in cyber security questions

Degree Master of Science in Economics and Business Administration

Master programme Accounting

Thesis supervisor Seppo Ikäheimo

Year of approval 2019 **Number of pages** 70 + 15 **Language** Finnish

Abstract

The main objective of this thesis is to research management responsibilities in terms of cyber security questions. In addition, this research aims to clarify how management and board understand different aspects that need to be considered in system projects.

The framework for the empirical part of this study was supported by Dutta & McCrohan (2002) since they had published same kind of conclusions that were research questions of this study. So, the framework started to evolve from what Dutta & McCrohan (2002) had published, but also the many meetings with different experts modelled the framework so that it would fit better for the purpose of this study. In theory, the framework that was developed, could be applied to information security/management responsibility theses in the future.

Interviews were conducted as case-type interviews and the organizations were scattered to different fields. Half of the organizations were service/industrial companies which were picked to represent the "traditional" industries whereas rest of the interviewed companies were advisory/consultant service companies.

Descriptive case study was the method that was picked for this study since the objective was to compare the similarities and divergencies of the phenomenon. In addition, because management responsibility questions and cyber security have not been researched that much abreast, this study has applied exploratory case study method as a secondary method. Exploratory method is often used when study pursues to find a new perspective to examine certain phenomenon and that's why there are two different methods in this study.

Based on the interviews, organizations encounter similar troubles in their daily business regardless of the field they operate. These were, to mention some, teaching new technology related skills and policies according to new information systems; communication and interaction between management and executing personnel; transforming decision making process to more participating form where more parties could be involved. Results also imply that management and board might not necessarily acknowledge the difference between the terms accountability and responsibility.

Keywords information security, cyber security, accountability, management

Aalto-yliopisto
Kauppakorkeakoulu

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi
Maisteritutkinnon tutkielman tiivistelmä

Tekijä Jere Rignell

Työn nimi Yritysjohdon vastuu/tilivelvollisuus yrityksen kyberturvakysymyksissä

Tutkinto Kauppatieteiden maisteri

Koulutusohjelma Laskentatoimi

Työn ohjaaja(t) Seppo Ikäheimo

Hyväksymisvuosi 2019 **Sivumäärä** 70 + 15 **Kieli** Suomi

Tiivistelmä

Tämän tutkimuksen päätavoitteena on tutkia yritysjohdon vastuukysymyksiä kyberturva-asioihin liittyen. Vastuukysymyksien tutkimisen lisäksi tutkielmassa pyritään selvittämään, millä tavalla ylin johto ymmärtää järjestelmähankkeita koskevat osa-alueet, ja pyrkiikö johto proaktiivisesti etsimään parempia ratkaisuja liiketoimintojen tehostamiseen järjestelmien näkökulmasta.

Tutkimuksen empiirisen viitekehyksen luomiseen haettiin tukea Dutta'n & McCrohan'n (2002) tekemän tutkimuksen kautta, sillä nämä tutkijat olivat julkaisseet samansuuntaisia tutkimustuloksia, joita tässä tutkimuksessa tutkittiin. Valinnan pohjalta tehtiin alustava viitekehys, jota alettiin muokata eri asiantuntijoiden näkemyksien pohjalta. Tapaamisten jälkeen syntyi tässä tutkimuksessa käytetty viitekehys, jota voisi teoriassa käyttää uusien kyberturvaa ja yritysjohdon vastuuta koskevien tutkimusten pohjana.

Haastattelut toteutettiin case-tyyppisinä haastatteluina, ja haastateltavat organisaatiot olivat hyvin erilaisilta aloilta. Puolet haastateltavista organisaatioista olivat palvelu- ja teollisuusalan yhtiöitä, jotka valittiin tutkimukseen edustamaan "perinteisiä" aloja, kun toinen puolisko organisaatioista koostui asiantuntija- ja neuvontapalveluita tarjoavista organisaatioista.

Metodina käytettiin kuvailevaa tapaustutkimusta, sillä tutkimuksessa pyrittiin selvittämään ilmiön olemusta samankaltaisuuksia ja eroavaisuuksia verraten. Lisäksi, koska yritysjohdon vastuukysymyksiä ja kyberturvallisuutta on tutkittu varsin vähän rinnakkain, on kuvailevan tapaustutkimuksen rinnalla käytetty tutkivan tapaustutkimuksen metodia. Tutkivan tapaustutkimuksen metodia käytetään usein, kun ollaan luomassa jotain uutta tapaa tarkastella tiettyä ilmiötä, ja tästä syystä myös tämä toinen metodi valittiin tutkimukseen.

Tutkimuksen perusteella organisaatiot kohtaavat hyvin samankaltaisia haasteita riippumatta toimialasta. Näitä olivat esimerkiksi uusien käytäntöjen ja tapojen opettaminen järjestelmiin liittyvissä asioissa; viestintä ylimmän johdon ja toteuttavan henkilöstön välillä; sekä mahdollisimman monen tahon osallistaminen päätöksentekoon organisaation operatiivisessa toiminnassa. Tutkimustulos myös viittaa yritysjohdon vastuun ja tilivelvollisuuden käsitteiden olevan jossain määrin epäselviä eikä niitä välttämättä ymmärretä täysin yritysjohdon keskuudessa.

Avainsanat tietoturva, kyberturva, tilivelvollisuus, ylin johto

Sisällysluettelo

1 Johdanto

Tietoturvakysymykset nousevat yhä suurempaan keskiöön yrityksen operatiivisessa toiminnassa. Mielenkiintoista on kysyä, millä tavalla yrityksen tietojärjestelmä tulisi rakentaa työntekijöiden, asiakkaiden ja muiden sidosryhmien näkökulmasta, jos samalla huomioidaan digitaalisempi yhteiskunta vuosikymmenien päästä? Tietojärjestelmien ja organisaation jatkuva kehittäminen lienee ilmeinen vastaus, mutta se ei kuitenkaan tarkoita, että organisaatiot investoisivat jatkuvasti uusiin järjestelmiin – pikemminkin tietojärjestelmäinvestointeja tehdään reaktiivisesti, kun yritysjohto esimerkiksi huomaa järjestelmien jääneen nykymaailman vaatimuksista. Organisaatioiden datan käsittely ja erilaiset tietovuodot ovat viime aikoina olleet otsikoissa, eikä näille uutisisille todennäköisesti näy loppua.

Regulaattorit ovat heränneet tähän haasteeseen asettamalla EU:n laajuisen tietosuoja-asetuksen (GDPR), joka tuli voimaan toukokuussa 2018. Asetuksen päätavoite on harmonisoida EU:n jäsenvaltioiden käsitystä henkilötietosuojasta. Käytännössä tämä tarkoittaa yritysten tarkempaa tiedonantovelvollisuutta ja tarkempaa käsittelyä näiden tietojen osalta. Tietosuoja-asetuksen voimaantulo on hyvä esimerkki siitä, miten organisaatioiden oli muututtava.

GDPR:n voimaantulo on viimeisin, mutta tuskin viimeinen asetus tietoturvaa ja kyberturvallisuutta koskien. Asioiden internet, biometrinen tunnistus sekä puettavat älylaitteet tuovat uusia mahdollisuuksia kuluttajille, mutta myös avaavat uusia mahdollisuuksia hyödyntää tietoturva-aukkoja hakkereiden toimesta. Tiedon kerääminen on aiempaa helpompaa ja yhä useammat osapuolet ovat valmiita maksamaan kerätystä datasta. On kuitenkin sanottu, että IoT-laitteet muodostavat seuraavien vuosien aikana suurimman tietoturva-uhan johtuen näiden laitteiden edullisuudesta, jolloin tietoturvaominaisuuksista todennäköisesti ensimmäisenä leikataan. Täten, dataa ei tulisi kerätä hinnalla millä hyvänsä, vaan vastuullisesti ja ihmisten yksityisyyden suojaa kunnioittaen.

Kyberturvallisuus ja sisäinen tarkastus – miten nämä liittyvät toisiinsa?

Aiemmin kyberturva ja yritysten tietoturva on nähty teknisenä ja teknologiaan liittyvänä asiana, jota voidaan parantaa parempaa teknologiaa ostamalla. Tässä näkemyksessä IT-osasto ja liiketoimintayksiköt ovat operoineet itsenäisesti ja tehneet sellaisia päätöksiä, joita ei oltaisi välttämättä tehty, jos IT-osasto ja liiketoimintayksikkö olisivat olleet vuorovaikutuksessa säännöllisesti järjestelmähankkeiden aikana. Viestintä ja yhteiset tavoitteet ovat mahdollisesti olleet hyvin kaukana toisistaan, mikä

on aiheuttanut ylipitkiä järjestelmähankkeita ja budjettien ylittymisiä prosessien ja yhteisten toimintatapojen ollessa puutteellisia.

Nykyisin tietoturva-asiat nähdään koko organisaatiota koskevana kokonaisuutena, johon vaikuttavat niin organisaation sisäiset toimintatavat kuin esimerkiksi kyberturvaan keskittyneiden yhtiöiden kanssa tehdyt tietoturvaharjoitukset ja näiden antamat suositukset organisaation tietoturvan tilasta. Lisäksi organisaation omat prosessit, tavat ja ihmisten kouluttaminen nähdään tärkeinä asioina, kun puhutaan organisaatioiden tietoturvasta ja sitä uhkaavista tekijöistä (Dutta & McCrohan, 2002).

Sisäistä tarkastusta käytetään edellä mainittujen asioiden löytämiseen ja tätä työtä tekevät ihmiset toimivat ”salapoliiseina” mahdollisten toimintaa vaarantavien tekijöiden etsimisessä. Tällöin sisäinen tarkastaja peilaa organisaation nykytilaa sen menneisyyteen. Sisäistä tarkastusta voidaan myös käyttää ennalta ehkäisevänä toimintana, jossa esimerkiksi vallitsevasta toimintakulttuurista pyritään löytää sellaisia tapoja jotka voivat vaarantaa organisaation toiminnan myöhemmin tulevaisuudessa. Tällöin sisäinen tarkastus toimii proaktiivisena työkaluna organisaation uhkien torjunnassa.

Mitä ovat tietoturva ja kyberturvallisuus?

Tutkimuksen aluksi olisi hyvä selvittää, miten tietoturva ja kyberturva eroavat toisistaan käsitteinä, ja miten ne toisaalta liittyvät toisiinsa. Valtavirrassa näitä käytetään usein toistensa synonyymeinä ja välillä ihmiset saattavat tietoturvasta puhuessaan tarkoittaa oikeasti kyberturvaa, mutta harvemmin toisinpäin. **Tietoturva** koskee kaikkia niitä järjestelyitä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus (Olin, ym. 2018). Tällöin kyse on teknologisista valinnoista, miten esimerkiksi joku tietovaranto on suojattu ulkopuolisten katseilta tai miten nopeasti yrityksen tarvitsemat tiedot ovat saatavilla järjestelmien kaatumisen jälkeen. Tietoturvalla tarkoitetaan arkisemmin ns. ”tiedon turvaamista” teknisin välinein. Tietoturva-käsite ei siten itsessään tarkoita muita asioita kuin niitä kyvykkyyksiä, joilla organisaatiot pyrkivät turvaamaan tietojen luottamuksellisuuden, eheyden ja saatavuuden.

Kyber- viittaa yleensä digitaalisessa muodossa olevan tiedon käsittelyyn, ja johon liittyy laajemmin koko tietoverkkoinfrastruktuuri sekä päätelaitteet, ohjelmistot ja käyttöjärjestelmät (Olin, ym. 2018). Kyber- on vastine sanalle digitaalinen (Limnéll, Majewski & Salminen, 2014). **Kybertuvallisuudella** yleisesti tarkoitetaan sellaista tavoitetilaa, jossa erilaisilla toimilla parannetaan kybertoimintaympäristön toimintamahdollisuuksia (Olin, ym. 2018). Organisaatioiden näkökulmasta näitä voisivat olla

esimerkiksi erilaisten prosessien ”parantuminen” tai esimerkiksi ihmisten kasvanut tietoisuus kyberturvauhista koulutuksen avulla.

Tietoturvan ja kyberturvan käsitteitä on käytetty tässä tutkielmassa mahdollisimman usein kuvaamaan ylläolevia tilanteita: tietoturvaa on käytetty, kun on käsitelty tiedon saatavuutta, eheyttä tai luottamuksellisuutta; ja kybertuvallisuutta silloin, kun käsiteltävä aihe ei koske pelkästään teknologiaan liittyviä asioita. Etukäteen on jo kuitenkin hyvä todeta, että näiden kahden käsitteen terminologinen eroavaisuus on niin huomattava, ettei lukijalle pitäisi tulla sellaista tilannetta, jossa hän voisi ymmärtää kontekstin väärin siinä käytetyn termin takia. Näitä kahta termiä on sen takia käytetty toistensa synonyymeinä, vaikka ne teoriassa tarkoittavatkin eri asioita.

1.1 Tutkimuskysymys & tutkimuksen tavoite & rajaus

Toimivan johdon ja hallituksen vastuuta yrityksen tietoturvakysymyksissä on tähän mennessä tutkittu akateemisesti lähinnä kyberturvallisuuden ja tietoturvan määrittelemisen näkökulmasta. Von Solms & van Niekerk (2013) perehtyivät määrittämään kyberturvallisuuden ja tietoturvan eroja sekä sitä, millä tavalla nämä ovat erotettavissa toisistaan ja millä tavalla ne kytkeytyvät toisiinsa. Von Solms & von Solms (2018) jatkoivat vuonna 2013 ilmestynyttä tutkimusta ja ottivat tähän tarkasteluun myös yritysjohdon ja hallituksen näkökulman.

Tämän tutkielman tarkoitus on perehtyä hallituksen vastuisiin yrityksen tietoturvakysymyksissä ja selvittää, miten ylin johto ymmärtää kyberturvallisuuteen liittyvät aiheet. Tutkielmassa tullaan käsittelemään seuraavia tutkimuskysymyksiä:

- Kuka on tilivelvollinen ja kuka on vastuussa oleva organisaation tietoturva-asioissa?
- Miten hallitus ja johtoryhmä ymmärtävät organisaation kyberturvallisuuden?

Tutkimuskysymyksiä on tarkasteltu kuvailevan tapaustutkimuksen avulla. Haastateltavat yritykset on rajattu koskemaan Suomen markkinaa ja haastateltavana on ollut ihmisiä yritysten johtoryhmistä, haastateltavan on ollut myös konsultteja sekä tietoturvasta vastaavia ihmisiä. Haastatteluissa on pyritty selvittämään ensinnäkin sitä, kuka tai ketkä ovat vastuussa tietoturvaa koskevista päätöksistä.

Lisäksi on pyritty selvittämään, onko hallitus toiminut reaktiivisesti vai proaktiivisesti etsiessään vastauksia yrityksen tietoturvan parantamiseksi.
Tutkimus on toteutettu case-tyyppisenä haastatteluna, jossa eri organisaatioiden tietoturvakäsitystä on vertailtu keskenään soveltuvin osin ja siten pyritty hakemaan kokonaisvaltaisempaa ymmärrystä näiden kohdeyhtiöiden tietoturvasta ja niiden riskien hahmotuskyvystä.

1.2 Tutkielman rakenne

Tutkielma koostuu viidestä pääluvusta, joista ensimmäinen (**Kirjallisuuskatsaus**) käsittelee tutkimusaihetta laskentatoimen teoreettisesta viitekehyksestä. Lisäksi kappaleessa esitellään **Organisaation turvallisuuden kolme komponenttia**, joita käytetään teoreettisena viitekehyksenä tämän tutkimuksen empiirisessä vaiheessa.

Toinen pääluku **Metodit & Data** käsittelee valittua metodia/metodeita sekä perustelee valintoja tutkimusaiheen avulla. Lisäksi kappale selittää tutkimuksen reliabiliteettia sekä validiteettia kerätyn datan avulla.

Kolmas pääluku **Tutkimustulosten raportointi** kuvailee haastatteluiden kautta saatua dataa, jotka on jaettu neljään alakohtaan (**Kriittinen infrastruktuuri, Organisaatio, Teknologia ja Ylin johto**). Nämä neljä alakohtaa ovat ensimmäisessä pääluvussa esitellyn viitekehyksen komponentteja, joiden avulla tutkimusaihetta on pyritty tutkimaan teoreetikon silmin.

Neljännessä pääluvussa **Keskustelu** vertaillaan jo tunnetun akateemisen tutkimuksen tuloksia tässä tutkimuksessa löydettyihin tuloksiin. Viimeisessä pääluvussa **Yhteenveto** kuvataan tutkimustulosta, käytännön merkitystä sekä mahdollisia jatkotutkimuksia.

Liitteessä yksi on lisätietoa kyberturvallisuudesta, joka antaa käytännön vinkkejä lukijalle turvallisemmasta arjesta. Liite kaksi ja kolme pitävät sisällään tärkeitä asioita tähän tutkimukseen liittyen. Liitteessä kaksi on esitelty kaikki kysymykset, joita haastatteluissa käytettiin. Liitteessä kolme on esitelty haastateltavat organisaatiot.

2 Kirjallisuuskatsaus

Kirjallisuuskatsaus on jaettu siten, että ensimmäiseksi käydään laskentatoimen näkökulmasta sisäistä tarkastusta ja tämän jälkeen siirrytään askel askeleelta kohti kyberturva-aihetta. Tutkija on tehnyt tietoisen valinnan jättäessään tutkimuksen tärkeimmän asian, eli kyberturvallisuuden ja tässä tutkimuksessa käytetyn viitekehyksen avaamisen, kirjallisuuskatsauksen loppuun. Loppujen lopuksi kyseessä on laskentatoimen pääaineen lopputyö ja tarkoituksena on näyttää nimenomaan laskentatoimea opiskeleville/sitä ymmärtäville ihmisille polku, miten nämä kaksi aihetta, laskenta ja tietoturva/kyberturvallisuus, liittyvät toisiinsa.

2.1 Sisäinen tarkastus

Sisäisellä tarkastuksella tarkoitetaan objektiivista, riippumatonta ja tiedollista menettelyä, jonka tarkoituksena on tuottaa lisäarvoa yritykselle paremman sisäisen ymmärtämisenä. Prosessien parempi tunteminen tuottaa siis lisäarvoa yritykselle. Sisäisellä tarkastuksella pyritään tutkimaan yrityksen riskienhallintaa, valvontaa, johtamis- sekä hallintoprosessien toimivuutta sekä näihin liittyviä tavoitteiden asettamista (Holopainen, ym. 2013).

Riippumattomuus ja objektiivisuus pyritään turvaamaan noudattamalla kansainvälisiä standardeja sekä toimintaa pyritään ohjata hyvien hallinnointitapojen ja johtamiskäytäntöjen avulla samalla eettisesti toimien. Standardien noudattaminen ja organisaation sisäinen hallintorakenteiden olemassaolo tulisi siten johtaa sisäisen tarkastuksen objektiiviseen ja riippumatomaan näkökulmaan. Seuraavaksi on lueteltu ne toimijat, joita sisäinen tarkastuksen avulla arvioidaan Holopaisen ym. (2013) mukaan:

- Hallitus
- Toimiva johto
- Sisäinen tarkastus
- Tilintarkastajat

Seuraavassa kappaleessa käsitellään tarkemmin edellä mainittujen toimijoiden vaikutusta sisäisen tarkastuksen toimittamiseen.

Sisäisen tarkastuksen toimijat

Hallitus: hallituksen vastuulla on huolehtia riskienhallinnasta ja valvonnasta niissä määrin, kuin mitä sen toimivaltaan on kirjattu. Hallitus voi käyttää apunaan erilaisia valiokuntia tavoitteiden saavuttamisen seuraamiseen sekä pyrkiä kohti parempaa tavoitteiden asettamista. Hallituksen toimintaa voidaan arvioida hyvän hallintotavan säännöillä (Holopainen, ym. 2013 & Prawitt, ym. 2009).

Toimiva johto: toimiva johto ja toimitusjohtaja hoitavat yrityksen operatiivista johtamista, johon kuuluu työn suunnittelu, organisointi, päätöksentekoa ja valvontaa koskevat tehtävät. Näihin tehtäviin lukeutuu myös strateginen ja operatiivinen suunnittelu ja implementointi, johtamis- ja hallintotehtävien toteuttaminen sekä riskienhallinnasta ja valvonnasta vastaaminen. Yksi tapa tarkastella johdon suoriutumista on tutkia johdon kykyä tuottaa osakkeenomistajille lisäarvoa (Holopainen, ym. 2013 & Prawitt, ym. 2009).

Sisäinen tarkastus: sisäistä tarkastusta toteuttaa sisäisen tarkastuksen johtajan lisäksi pieni tiimi organisaation ulkopuolelta, jonka tehtävänä on tutkia organisaation sisäisiä hallinnointijärjestelmiä ja antaa näiden löydösten perusteella konsultointia yritysjohdolle. Sisäisen tarkastuksen toimittamista voidaan arvioida kansainvälisten kriteerien perusteella (Holopainen, ym. 2013 & Prawitt, ym. 2009).

Tilintarkastajat: Tilintarkastajat toteuttavat organisaatioiden lakisääteisen tilintarkastuksen. Tilintarkastajien toimintaa voidaan arvioida tilintarkastajien työtä koskevan lainsäädännön kautta (Holopainen, ym. 2013 & Prawitt, ym. 2009).

2.2 Riskienhallinta

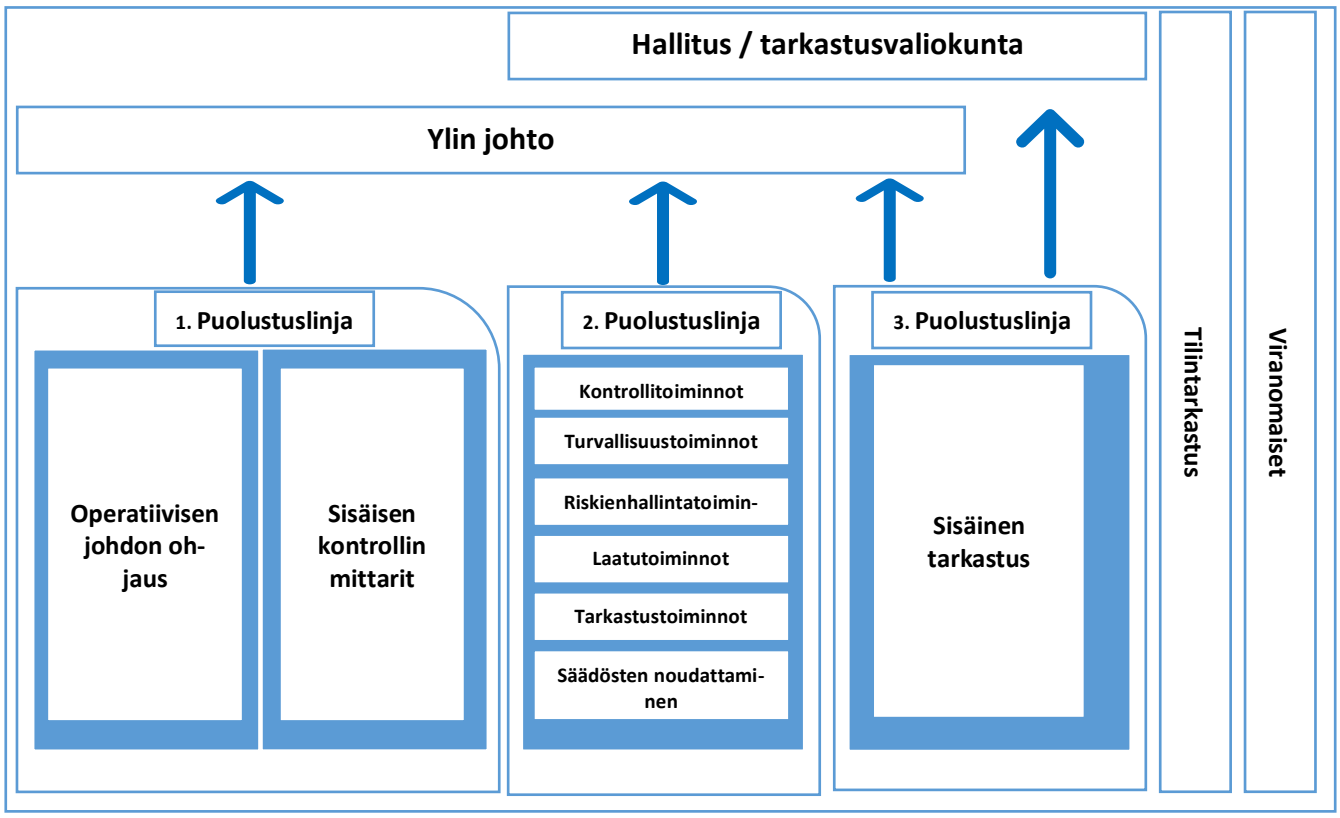
Organisaatioissa on nykyään monen alan asiantuntijoita hoitamassa sisäistä valvontaa: sisäisiä tarkastajia, laatutarkkailijoita ja selvitysmiehiä selvittämässä johdon toimia ja niin edelleen. Nämä erillisissä tiimeissä toimivat ihmiset tutkailevat kuitenkin samaa asiaa hyvin erilaisten silmälasien läpi, ja heillä saattaa myös olla erilaiset kyvykkyydet. Tästä syystä organisaation kannalta olisi tarkoituksenmukaisempaa, jos nämä eri lähtökohdista toimien tiimien vastuunjako ja koordinointi on tehokasta. Jokaiselle tiimille asetetaan rajattavissa oleva vastuualue, mitattavissa oleva päämäärä ja osatavoitteet, miten maaliin päästään.

Riskienhallintaa voidaan pitää yhtenä organisaation olemassaoloa ylläpitävistä voimista. Jotta riskienhallinta toimisi, tulisi organisaation määritellä ja tunnistaa mahdolliset riskit ja mahdollisuudet

jollakin systemaattisella menetelmällä, ja tähän todennäköisin varautumisen muoto on tarkoituksenmukainen ja ajassa elävä riskienhallintajärjestelmä (Holopainen, ym. 2013).

Kolme puolustuslinjaa

Kolmen puolustuslinjan asetelma tarjoaa tehokkaan tavan jakaa vastuualueita organisaation sisällä huolimatta organisaation koosta. Ylintä johtoa ja hallitusta ei varsinaisesti lueta näihin kolmeen linjaan, sillä puolustuslinjojen tarkoitus on tukea heitä päätöksenteossa. Lisäksi, puolustuslinjojen tehtävä on palvella omistajia ja muita sidosryhmiä (IIA, 2013).



Kuvio 1: Kolmen puolustuslinjan asetelma.

Ensimmäinen puolustuslinja: operatiivinen johto hallinnoi riskiä päivittäin. Operatiivisen johdon tarkoitus on tutkia, tunnistaa ja tarkkailla mahdollisia riskejä sekä pyrkiä pienentämään riskikeskittymiä samalla ohjaten organisaatiota kohti asetettuja tavoitteita. Kontrollit ja varmistus on perinteisesti sisällytetty johdon päivittäisiin rutiineihin, jolloin ensimmäinen linja toimii tehokkaana riskien seulojana (IIA, 2013).

Toinen puolustuslinja: tukee ensimmäisen puolustuslinjan toimintoja. Johdon vastuulla on perustaa ensimmäistä linjaa tukevat riskinhallintamekanismit ja säädöstenmukaisuutta monitoroivat toiminnot. Jokaisella toiminnolla on jonkin asteinen riippumattomuus ensimmäisen linjan toiminnoista, ja koska niillä on selkeä linkki johdon rutiineihin, ne eivät pysty antaa täysin riippumatonta kuvaa johdolle toiminnon vaikutuksesta. Kyseiset toiminnot voivat vaihdella organisaatiosta riippuen (IIA, 2013).

Kolmas puolustuslinja: sisäisen tarkastuksen linja, jossa pyritään tarjota riippumatonta kolmannen osapuolen näkemystä organisaation prosesseista. Puolustuslinjaa voidaan toteuttaa myös organisaation sisältä käsin, mutta tällöin nämä ihmiset eivät saisi olla tekemisissä ensimmäisen tai toisen puolustuslinjan kanssa riippumattomuuden turvaamiseksi. Sisäisen tarkastuksen perustaminen ennen kaikkea pieniin yrityksiin mahdollistaa pienen toimijan keskittymisen (IIA, 2013).

2.3 Tietojärjestelmät sisäisen tarkastuksen kohteena

Tietojärjestelmätarkastuksiin liittyy kaikki ne toiminnot, jotka auttavat arvioimaan tietojärjestelmää, sen valvontaa ja johtamista. Tietojärjestelmää tarkastelevilla toiminnoilla pyritään arvioimaan neljän kriteerin perusteella. Pyritään vastata, onko järjestelmällä kyky (Holopainen, ym. 2013):

1) turvata organisaation omaisuus
2) varmistaa tietojen oikeellisuus, saatavuus ja toimintojen jatkuvuus
3) säilyttää tietovarantojen eheys
4) asetettujen tavoitteiden mahdollisimman tehokkaaseen ja taloudelliseen saavuttamiseen

Sisäinen tarkastus on varsin säännöstelemätön funktio, josta johtuu, että sisäisen tarkastuksen fokus saattaa vaihdella suuresti ja tarkastettavat kohteet pyrkivät vastaamaan sen hetken operatiiviseen tarpeeseen (Prawitt, ym. 2009). Sisäisen tarkastuksen funktio voi toimia operatiivisen, kontrollien tai systeemien tarkastajana riippuen johdon tarpeista (esim. Anderson, 1996; Klinkerman, 1996; Thevenin, 1997).

Tarkastuksen lähtökohtana on arvioida tietojärjestelmää kokonaisvaltaisesti. Tähän tarkastelun piiriin kuuluvat siten kaikki tietojärjestelmän osa-alueet organisaation koko elinkaarelta: palvelintilan, tur-

vallisuuden, toipumisen ja jatkuvuuden valmiudet sekä sovellukset ja niiden kehittämisen tarkastukset. Tietojärjestelmä tarkastuksissa törmää usein Cobit-termiin, joka on yleinen viitekehys tietojärjestelmien hyvään hallinnointitapaan liittyvä koodisto. Koodiston on luonut ISACA (kansainvälinen tietojärjestelmätarkastuksen katto-organisaatio), joka antaa ohjeistuksia sisäisille tarkastajille helpottamaan hyvän hallinnointitavan arviointia (Holopainen, ym. 2013).

Cobit-malliperheeseen kuuluu useita erilaisia ammattiohjeita, jotka tutkivat tietojärjestelmiä niiden riskin ja hyvän hallinnointitavan näkökulmasta. Nämä ammattiohjeet rakentuvat kuuden pääperiaatteen mukaan (ISACA, 2018):

1) Arvonluominen sidosryhmille
2) Kokonaisvaltainen lähestyminen
3) Dynaaminen hyvä hallinnointitapa
4) Hallinnon ja johtamisen eriyttäminen
5) Räätälöinti yritystarpeen mukaan
6) Yritystoimintojen kattaminen koko elinkaaren osalta

2.3.1 Hyvä johtamis- ja hallinnointitapa tietohallinnassa

IT-järjestelmä on kokonaisuus, jota on haastavaa tarkastaa ja arvioida, sillä se on yhteydessä hyvin moniin eri funktioihin organisaatiossa. Tietojärjestelmää tarvitaan niin operatiivisen liiketoiminnan pyörittämisessä kuin strategisessa tavoitteiden asettamisessa ja näiden tavoitteiden seurantaan liittyvissä asioissa. Lisäksi voidaan sanoa, että tietojärjestelmä voi joko auttaa saavuttamaan paremman kilpailuasetelman tai heikentää nykyistä tilaa entisestään.

2.3.2 Liiketoiminnan ja tietohallinnon välinen vuoropuhelu

Holopaisen ym. (2013) mukaan IT ja tietohallinto kuuluvat samaan kokonaisuuteen, josta vastaa hallitus ja ylin johto. Hallituksen tavoitteena on kirkastaa IT-projektien tavoitteet siitä vastaavalle henkilöstölle, jotta nämä osaisivat omilla toimillaan toteuttaa tätä tavoitetta päivittäin. Erityisen kriittistä

on ymmärtää IT-hankkeisiin liittyvät riskit ja niistä saatava hyöty. Tämän takia hallituksen tulisi pyrkiä vuoropuheluun tietohallinnon henkilöstön kanssa mahdollistaakseen tarvittavan ymmärryksen näiden kahden välillä, ja jotta hallituksen tavoitteet saataisiin kirkastettua myös IT-henkilöstön päivittäiseen toimintaan. Tällöin kommunikoinnin merkitys nousee tärkeäksi osatekijäksi, kun vertaillaan asetettujen tavoitteiden ja saavutettujen tulosten välistä eroa.

Huomattava määrä tieteellisestä tutkimuksesta on havainnut, että IT-funktiota ja liiketoimintayksiköitä pidetään hyvin erillisinä toimintoina. Siurdyban'n (2014) mukaan tämä luo kuvitteellisia ja siilomaisia rakenteita organisaatioihin, mikä itsessään luo epäjatkuvuutta ja kitkaa eri funktioiden välille. Ja koska IT-funktiossa tehdyt päätökset vaikuttavat koko organisaatiossa, IT-osaston vaikutusvalta sekä suhteet eri toimintojen välillä tulisi organisoida siten, että se heijastelisi paremmin tätä IT-osaston asemaa koko organisaatiossa.

Johdon tehtäviin IT-asioiden suhteen on tarjota vaadittava IT-infrastruktuuri, jonka avulla organisaatio pystyy osoittaa vastuualueet, niiden jakamisen ja organisoinnin sekä mitata tavoitteiden saavuttamista. Erillisen tiimin perustaminen strategisten tavoitteiden saavuttamisen suhteen voi tulla tarpeeseen, mutta tiimin tulisi huolehtia myös tarvittavien taitojen harjoittamisesta muulle henkilöstölle sekä riskien ja kontrollien hallinasta. Vastavuoroisesti IT-tiimin tulisi pyrkiä keskustelemaan tavoitteiden asettamisesta hallituksen ja ylimmän johdon kanssa ja suositella parannuksia tehtyyn strategiaan (Holopainen, ym. 2013 & Siurdyban, 2014).

2.3.3 Tietohallinnon perusratkaisuja

Tietohallinnon järjestämisessä voidaan käyttää joko hajautettua tai keskitettyä tietohallinnon järjestämistapaa tai sitten näiden yhdistelmää, jolloin osa toiminnoista hoidetaan hajautetusti ja osa keskitetysti. Äärimmäinen hajautuksen muoto on loppukäyttäjän tietotekniikka, jolloin loppukäyttäjä huolehtii tietojärjestelmistä ja niiden hallinnosta itsenäisesti. Kyseiset toiminnot voidaan myös ostaa ulkopuolisena palveluna, jolloin ulkopuolinen toimittaja hoitaa organisaation tietohallinnon. Järjestämiseen liittyvien kysymysten tärkein periaate on järjestää toiminnot niin, että ne ovat tarkoituksenmukaisia ja organisaation asettamien tavoitteiden mukaisia (Holopainen, ym. 2013).

Keskitetty tietoratkaisu

Keskitetyn tietoratkaisun etuina voidaan pitää laiteinfrastruktuurin helpompaa hallintaa ja valvontaa, sillä usein tietojärjestelmät sijaitsevat usein lokaalisti keskitetyssä tietoratkaisussa. Lisäksi etuina ovat tietoturvaa koskevien kontrollien parempi suorittaminen, sovelluskehityksen ja laitteiston tuoma tehokkuus standardoinnin suhteen (Holopainen, ym. 2013 & Kim, ym. 2013).

Keskitetyn tietoratkaisun haittapuolina voidaan pitää laitteistoriippuvuutta yhdestä käyttöjärjestelmästä, mahdollisesta tietojen siirrosta aiheutuvat korkeammat kustannukset sekä suurempi lokaaliin sijaintiin liittyvä riski esimerkiksi tulipalon tai vesivahingon sattuessa (Holopainen, ym. 2013 & Kim, ym. 2013).

Hajautettu tietoratkaisu

Hajautetun tietoratkaisun etuina voidaan pitää tietojen hajauttamista serverien eri sijaintien avulla useaan eri kohteeseen, jolloin esimerkiksi tulipalon tai vesivahingon aiheuttama tietojen kokonaisvaltainen häviäminen voidaan välttää. Lisäksi, käyttäjät voivat kontrolloida sovelluskehittämistä paremmin, sillä muutoksiin voidaan reagoida nopeammin ja virheenkäsittely tehostuu sovelluskehityksen eri vaiheissa. Etuina voidaan pitää myös liiketoimintajohtajan parempaa näkyvyyttä tietohallinnon aiheuttamiin kustannuksiin sekä tietoturvaa koskevaa parempaa ulkoisen uhan torjumisvalmiutta (Holopainen, ym. 2013 & Kim, ym. 2013).

Hajautettu tietohallinnon ratkaisu tekee järjestelmän hallinnasta monimutkaisempaa ja prosessien standardointiin liittyvät tehostamismahdollisuudet heikkenevät sekä kontrollien suorittaminen hankaloituu. Lisäksi, tietohallinnon järjestämiseen voi liittyä monia käyttöjärjestelmiä, jolloin näihin tehtävät samanaikaiset päivitykset ja yhteensopivuusongelmat lisääntyvät (Holopainen, ym. 2013 & Kim, ym. 2013).

Loppukäyttäjän tietotekniikka

Vastuu järjestelmän kehittämisestä voidaan myös vyöryttää loppukäyttäjän harteille, jolloin hän vastaa esimerkiksi sovelluskehittämisestä ja niiden testaamisesta. Tästä esimerkkinä on monien organisaatioiden käyttämä Excel-laskentajärjestelmä, jossa Microsoftin kehittämää laskentatyökalua käytetään esimerkiksi organisaation hankintojen ja muiden kustannuksia aiheuttavien toimintojen seuraamiseen (Holopainen, ym. 2013 & Kim, ym. 2013).

Etuina loppukäyttäjän tietotekniikassa voidaan pitää sovellusten räätälöintiä käyttäjää kohden juuri siihen tarkoitukseen kuin käyttäjä itse haluaa sovellusta käytettävän. Suurin haaste kuitenkin liittyy juuri käyttäjän omaan taitotasoon: osaako käyttäjä hallinnoida ja testata itse kehittämäänsä ohjelmaa. Käyttäjällä voisi esimerkiksi olla tarvittava taitotaso luoda laskentajärjestelmä itse, muttei valmiuksia vastata riskeistä tai tarvittavasta dokumentoinnista (Holopainen, ym. 2013 & Kim, ym. 2013).

Ulkoistettu tietojenkäsittely

Tietohallinnon ylläpitäminen voidaan myös ulkoistaa tietohallinnoista vastaavan organisaation vastuulle, jos ulkoistava osapuoli pyrkii esimerkiksi tehostamaan ja keskittämään omia operatiivisia toimintoja. Tärkeänä kysymyksenä on tällöin määrittää, vastaavatko ulkoistamiseen liittyvät asiat johdon asettamia tavoitteita ja onko näillä ratkaisuilla organisaation näkökulmasta kilpailukykyä tehostava vai haittaava vaikutus. Ulkoistamisen etuina on organisaation lisääntynyt tehokkuus ja keskittyneisyys sekä mahdollinen toimittajan ja ulkoistavan osapuolen tiiviimpi yhteistyö (Holopainen, ym. 2013 & Rustagi, ym. 2008).

Ulkoistaminen usein lisää riippuvuutta ulkoisesta toimittajasta, jolloin toimittajan ongelmat heijastuvat ulkoistavan organisaation ongelmiksi. Ulkoistavan osapuolen on myös usein haastavaa irtautua nykyisestä sopimussuhteesta, sillä organisaation keskittyminen omiin liiketoimintoihin usein aiheuttaa IT-toimintojen ammattitaidon asteittaisen katoamisen organisaation sisältä. Ongelmatilanteessa kustannukset kohoavat tiedon siirtämisen takia tai toimittajan vaihtamisen vuoksi, jos mahdollisen exit-tilanteen suunnitelmaa ei ole laadittu ulkoistamispäätöstä tehdessä. Lisäksi toimittajalla harvemmin on asiakkaidensa ammattitaitoa näiden omista liiketoiminnoista, jolloin lisäarvon tuottaminen tietohallinnon järjestämisen kautta heikkenee (Holopainen, ym. 2013 & Rustagi, ym. 2008).

2.3.4 Tietoturvapolitiikka ja ohjeistaminen

Organisaatio tiedottaa tietoturvapolitiikastaan julkisissa lähteissä, ja ne löytyvät vuosikertomuksesta tai muusta sähköisestä lähteestä kuten organisaation verkkosivuilta. Näiden periaatteiden sisältö harvoin on kovin konkreettinen, sillä tietoturvapolitiikan on tarkoitus antaa yleisiä suuntaviivoja organisaation tietoturvasta. Lisäksi tietoturvapolitiikkaa ja ohjeistuksia koskevaa kirjallisuutta ei juurikaan ole, vaan tutkimus on fokusoitunut erilaisten järjestelmien testaamiseen kuten Herath, ym. (2009) myös toteavat.

Holopainen, ym. (2013) kuvaavat, että tietoturvapolitiikkaan ja ohjeistuksien antamiseen sisältyy myös organisaation valtuutuksiin liittyviä asioita. Ohjeistus jakaantuu seuraaviin alakohtiin: yleiset tietoturvaperiaatteet, tietojen luokittelu, henkilöstön toimivaltuudet työpaikalla ja etätöissä, verkossa toimimisen ohjeet ja hallinnollinen turvallisuus. Käsitellään näitä yksityiskohtaisemmin seuraavaksi.

Yleiset tietoturvaperiaatteet

Johdon ja tietohallintovastaavan tehtäviin kuuluu laatia yhteiset suuntaviivat, joita koko organisaation tulisi noudattaa. Näihin suuntaviivoihin kuuluu tietoturvan ja organisaation strategian kohtaaminen sekä tietoturvalle asetettujen tavoitteiden laatiminen. Lisäksi tulee määrittää tietoturvan soveltamisalat, vastuualueet ja työtehtävien delegaatio organisaation muita tavoitteita vastaavaksi. Näillä tietoturvaperiaatteilla on usein myös ilmoitettu voimassaoloaika sekä tiedonantopolitiikka (Holopainen, ym. 2013).

Tietojen luokittelu

Tiedon luokitteluperiaatteet ovat organisaation näkökulmasta hyvin keskeinen tietoturvan osa-alue. Ensinnäkin ne kertovat henkilöstölle, että millaista tietoa organisaatio käsittelee sekä tekee salassa pidettävien tietojen ja julkisten tietojen käsittelystä erilaisten työtehtävien mielessä näkyvämpää (Andreasson, ym. 2015). Tietojen luokittelu vaikuttaa muun muassa siihen, miten tietoa voidaan käsitellä ja jakaa: voiko tietoa kopioida ja liittää tai lähettää postilla, ja lisäksi tulisi päättää miten tietoa säilytetään (Holopainen, ym. 2013).

Henkilöstön toimivaltuudet työpaikalla ja etätöissä

Organisaation tulisi kuvata valtuutuksiin liittyvä byrokratia mahdollisimman tarkoituksenmukaisesti: kenellä on ylin vastuu ja velvollisuus huolehtia käyttöoikeuksien myöntämisestä, milloin tiedot näistä käyttöoikeuksista poistetaan ja millaisia ongelmia näihin eri tilanteisiin voisi liittyä. Periaatteena yleensä käytetään ”least privilage”-käyttöoikeutta, jossa henkilöstölle myönnetään vähäisimmät oikeudet oman työnsä tekemiseen. Tällöin vältetään turhaa ylläpitäjän käyttöoikeuksien käyttöä, jolloin vähennetään riskiä aiheuttaa käyttöoikeuksiin liittyviä väärinkäyttöjä (Holopainen, ym. 2013).

Työpaikalla ja etätöissä tulisi olla erilaiset työntekoon liittyvät luokittelut, mitä töitä voidaan suorittaa työpaikan ulkopuolella ja millä valtuutuksilla näitä töitä tehdään. Yleisesti organisaation kannattaa

harkita mahdollisimman tiukkaa politiikkaa etätöiden tekemiseen ja määritellä hyvin tarkasti, millä laitteilla ja missä laiteympäristöissä töitä voidaan tehdä. Organisaation turvallisuuden kannalta tiukka valtuutuspolitiikka esimerkiksi laitteen hukkumisen tapauksessa etätöissä voi parhaassa tapauksessa johtaa ainoastaan laitteen nimellisarvon suuruiseen menetykseen (Holopainen, ym. 2013).

Netissä toimimisen säännöt

Ihmisen työidentiteetti harvoin jää pelkästään koskemaan omaa työyhteisöään ja työpaikkaa työpäivän päätteeksi, vaan identiteetti säilyy myös vapaa-ajalla. Tästä syystä organisaation tulisi määritellä verkkokäyttäytymisen säännöt eli miten ihmiset saavat käyttäytyä sosiaalisessa mediassa, kun he näyttäytyvät yksityishenkilöinä ja miten käyttäytyä, kun he näyttäytyvät organisaation edustajina. Netissä toimimisen sääntöjä on saatavilla useista verkkolähteistä ja näitä kannattaa hyödyntää omassa tietoturvapolitiikassaan. Netin sääntöjen tulisi sisältää ohjeita ihmisten vastuualueista esimerkiksi, miten viestintä sidosryhmille hoidetaan ja kuka tästä vastaa (Holopainen, ym. 2013).

Hallinnollinen turvallisuus

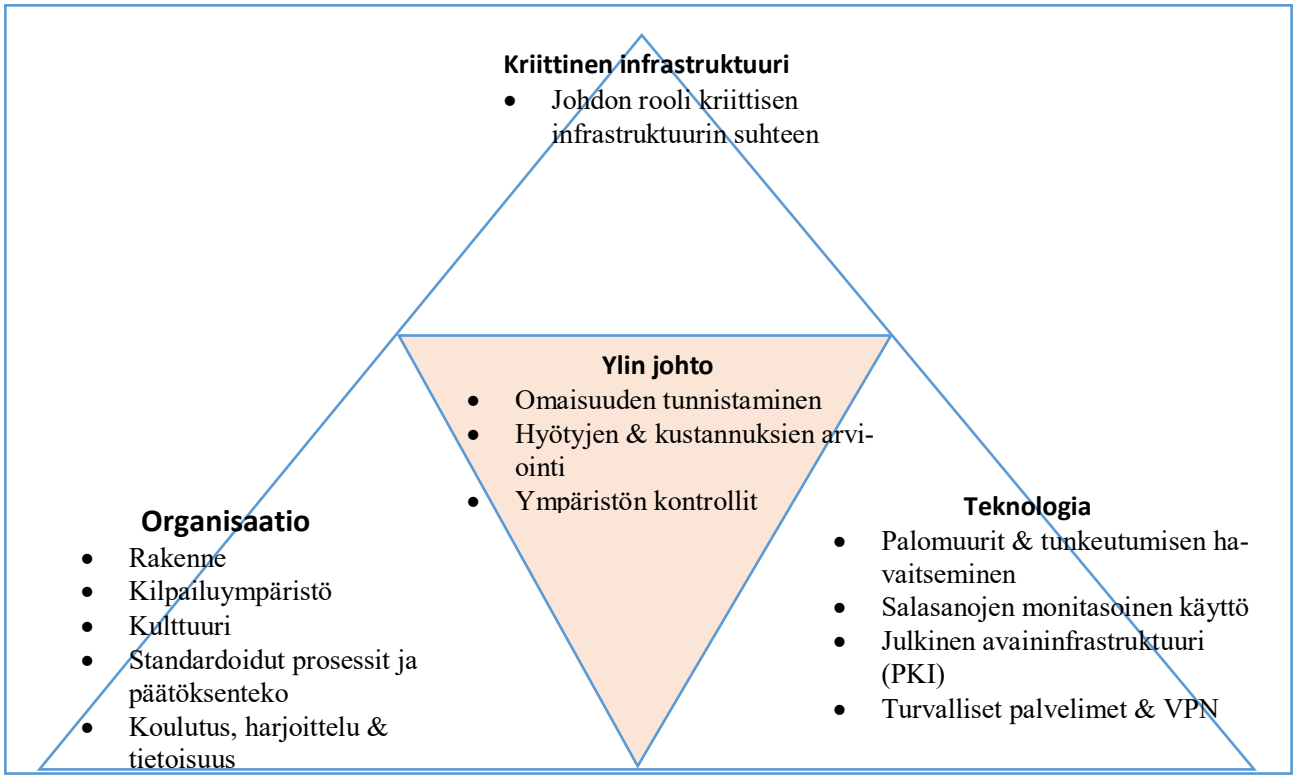
Hallinnolliseen turvallisuuteen lukeutuu kaikki ne toimenpiteet, joilla ohjataan, valvotaan ja organisoidaan tietohallinnon turvallisuuteen vaikuttavia tekijöitä. Näihin lukeutuu yleiset turvallisuuteen lukeutuvat järjestelyt, tehtävien delegaatio sekä koulutuksien järjestäminen tietoturvallisuuteen liittyvissä asioissa (Holopainen, ym. 2013). Hallinnollinen turvallisuus on siten organisaation turvallisuuteen liittyvien osatekijöiden koossa pitävä elementti.

2.4 Johdon rooli yrityksen kyberturvallisuudessa

Internet-pohjainen kaupankäynti on helpottanut monien toimijoiden asiointia, sillä enää palvelut ja tavarat ei ole paikkaan sidottuja eikä organisaatioilla ole tarvetta toimia ainoastaan kotimarkkinoilla. Samalla kun uudet mahdollisuudet ovat luoneet uusia ideoita ja on syntynyt uusia yrityksiä, on syntynyt myös uusia uhkia niin asiakkaita, toimittajia kuin muita sidosryhmiä kohtaan (Dutta & McCrohan, 2002).

Kyberturvakysymysten ymmärtäminen lähtee organisaation ylimmiltä tasoilta, miten hallitus esimerkiksi näkee yrityksen kyberturvan ja siihen liittyvät uhat sekä millä tavalla tähän liittyviä tavoitteita asetetaan ja miten näitä tavoitteita mitataan (Dutta & McCrohan, 2002). Lisäksi, kuten riskienhallinta pääluvussa mainittiin, myös kyberturvallisuuteen liittyvien järjestelmien tulisi pystyä elää ajassa (Holopainen, ym. 2013).

Tässä kappaleessa pyritään käsittelemään Dutta'n & McCrohan'n (2002) viitekehyksen perusteella organisaation rakenteisiin ja johtamistapaa koskevaa lähestymistä. Viitekehys perustuu kolmeen pääpointtiin, joiden keskiössä on yritysjohdon toiminta: kriittinen infrastruktuuri, organisaatio ja teknologia. Viitekehyksen avaamisen perusteella luodaan pohja tutkimuksen empiiriselle kolmannelle osiolle. Ennen tätä määritellään kuitenkin muutamia keskeisiä konsepteja kyberturvallisuuden suhteen.



Kuvio 2: Organisaation turvallisuuden kolme komponenttia (Dutta & McCrohan, 2002).

Turvallisuus ja yksityisyys: käsitteiden eroavuus voidaan määritellä organisaation ja sidosryhmän välisen vuorovaikutuksen kautta, jossa organisaation on tiedon ylläpitäjä ja sidosryhmän toimija on tietoa antava entiteetti. Yksityisyyden uhasta puhutaan silloin, kun organisaatiolla on sidosryhmän tietoja yli sen oman tarpeen tai jos monista vapaasti saatavista lähteistä saatua tietoa yhdistelemällä voidaan saada yksilön yksityisyyttä loukkaavia tietoja. Turvallisuuden uhasta puhutaan silloin, kun ulkopuolinen toimija pyrkii ylittämään sille suodun toimivallan saatavilla olevan tiedon suhteen. Tämä tarkoittaa siis sitä, että organisaatio käsittelee ulkopuolelta tulevia uhkia omassa toiminnassaan,

joiden tarkoituksena on saada organisaation järjestelmistä tietoa sen sidosryhmistä (Dutta & McCrohan, 2002).

Tietojärjestelmäinvestoinnit ja kannattavuus

Tietojärjestelmäinvestointien vaikutusta yrityksen tulokseen pidetään negatiivisen tulosvaikutuksen takia paljon taustatutkimusta ja selvitystä vaativana, sillä tietojärjestelmiä koskevaa vaikutusta on hyvin haastavaa mitata. Esimerkiksi tilikauden tulokseen tietojärjestelmäinvestoinnit vaikuttavat niistä tehtävien poistojen verran, jolloin aineettomiin hyötyihin kuten organisaation tehokkuuteen, ei välttämättä voida ottaa kantaa. Aineettomat hyödyt on vaikea kääntää numeroiksi, mutta asiakastyytyväisyyden turvaamiseksi tietojärjestelmäinvestoinnit ovat välttämättömiä (Dutta & McCrohan, 2002).

Turvallisuus uhattuna

Internet-pohjainen kaupankäynti lisää uhkia ylimmän johdon, johtamiskulttuurin sekä yritysrakenteen suhteen. Jos organisaatio esimerkiksi hankkii sofistikoitunutta teknologiaa ja jonka tulisi nostaa organisaation kyberturvatilan uudelle tasolle, ei asetettuja tavoitteita tulla saavuttamaan, jos henkilöstö ei ole oppinut käyttämään sitä oikein. Lisäksi uutta IT-henkilöstöä palkatessa katsotaan heidän ansaitsemia sertifikaatteja ja kunniamainintoja, mutta ei esimerkiksi taitoa opettaa näitä asioita muulle henkilöstölle.

2.4.1 Kriittinen infrastruktuuri

Kriittinen infrastruktuuri on ensimmäinen Duttan & McCrohanin (2002) esittelemän viitekehyksen kulmakivistä, jonka päälle rakentaa vankka tietoturvaperusta. **Kriittiseksi infrastruktuuriksi** määritellään sellaiset järjestelmät, joiden vahingoittaminen aiheuttaisi huomattavia fyysisiä tai taloudellisia seurauksia organisaatioille. Näihin toimialoihin luetaan esimerkiksi televiestintä-, energia- ja pankkiala. Yleisesti kriittinen infrastruktuuri on omistettu yksityisin varoin, vaikka näitä käyttää sekä julkiset että yksityiset toimijat (Dutta & McCrohan, 2002). Seuraavassa kappaleessa kuvataan johdon roolin vaikutuksia erilaisissa kriittiseen infrastruktuuriin liittyvissä asioissa.

Johdon rooli kriittisen infrastruktuurin suhteen

Yksityisellä ja julkisella sektorilla on hyvin erilaiset tavoitteet organisaation voiton tavoittelun suhteen, sillä yksityisten yritysten tarkoitus on useimmiten tuottaa voittoa omistajilleen, kun taas julkisella organisaatiolla voi olla myös muita tavoitteita kuten tuottaa yleishyödyllisiä palveluita yhteiskuntaan. Lisäksi näillä eri sektorin toimijoilla voi olla hyvin erilaiset kulttuuriset perinteet (Dutta & McCrohan, 2002).

Luottamuksen rakentaminen yksityisen ja julkisen sektorin välille on ollut haastavaa, vaikka luottamussuhteen syntymiselle olisi selkeitä hyötyjä. Ensinnäkin, luottamussuhteen muodostuminen vaatii organisaation henkilöstön sitoutumista muutokseen sekä rahoitusta, jotka molemmat ovat niukkoja molemmilla sektoreilla. Toiseksi, luottamussuhteiden ylläpitäminen on yleisesti haastavaa, sillä ne vaativat organisaation jatkuvia resursseja sekä paneutumista pitkän aikavälin luottamussuhteen ylläpitämiselle. Lisäksi, kahden erilaisista lähtökohdista tulevien organisaatioiden yhteensovittaminen vaatii hyvää johtamista, joka ottaa huomioon julkisen ja yksityisen sektorin erilaiset kulttuurit, tavat ja uskomukset (Dutta & McCrohan, 2002).

Suhteen syntymisen hankaluus nimenomaan liittyy organisaatioiden erilaiseen suhteutumiseen investointeihin: yksityisomisteisella yrityksellä usein tiukka tulosvastuu, kun taas julkisen organisaation löyhempi suhteutuminen voiton tavoitteluun asettaa eri sektorien toimijat eriarvoiseen asemaan. Suhteen muodostamiselle on kuitenkin olemassa selkeät hyödyt: tietoturvaan liittyvien kustannuksien pieneneminen yhteisten turvallisuusratkaisujen muodossa, ja lisäksi organisaatiot voivat yhteistyössä määritellä tietoturvan vaikutukset taloudellisesta näkökulmasta. Tämä johtaa parhaiden toimintatapojen evoluutioon, jossa parhaat ratkaisut niin tehokkuuden kuin taloudellisuuden näkökulmasta, syrjäyttävät huonosti toimivat ja taloudellisesti perustelemattomat hankkeet. Sektorien tekemä yhteistyö myös auttaa muovaamaan organisaatioiden hallinnollisia rakenteita sekä lainsäädäntöä parhaita käytäntöjä suosivaksi (Dutta & McCrohan, 2002). Lopuksi, yhteistyö lisää organisaation tunnistettavuutta hallinnollisen toimijan asiakkaiden silmissä sekä lisää yksityisen johdon ymmärrystä julkisen organisaation toimintatavoista (NDIA, 2000).

Ylimmän johdon vastuulla on tunnistaa kriittisen infrastruktuurin merkitys hyvien hallinnointitapojen suhteen, ja lisäksi tunnistaa kriittisen tiedon turvaaminen yli organisaation omien toimivaltuuksien. Ylimmän johdon vastuulla on myös tarjota johtajuutta, jossa huomioidaan julkisen ja yksityisen sektorin erilaiset kulttuuriset ja rakenteisiin liittyvät asiat, jotta nämä kahden eri sektorin edustajat saataisiin tekemään yhteistyötä (Dutta & McCrohan, 2002).

2.4.2 Organisaatio

Organisaatio on Dutta'n & McCrohan'n (2002) esittelemän viitekehyksen toinen kulmakivi, jonka päälle johto voi rakentaa ymmärtämällä organisaation sisäisiä asioita ja siihen liittyviä ulkoisia tekijöitä. Organisaatiot rakentuvat ihmisten välisistä suhteista ja monilla organisaatioilla on paljon yhtäläisyyksiä, kun vertaillaan eri organisaatioita keskenään. Näistä merkittävimmät ovat organisaatiorakenne, kilpailuympäristö, kulttuuri, standardoidut prosessit ja päätöksenteko. Näistä jokainen vaikuttaa organisaation turvallisuuteen ja siksi niiden ymmärtäminen on tärkeää (Dutta & McCrohan, 2002). Käsitellään näitä seuraavaksi.

Organisaatiorakenne

Onko organisaatiolla selkeä vastuunjako tietoturvaan liittyvistä asioista? Jos esimerkiksi ei ole mitään selkeää rakennetta tietoturvan vastuualueiden suhteen, tämä saattaa johtaa tietoturvariskien kasvamiseen. Jos esimerkiksi yrityksessä tehdään jokin uusi tietoturvaan liittyvä parannus, sen toimeenpano voi olla tehotonta, jos henkilöstöä ei onnistuta informoimaan muutoksista.

Liiketoimintojen ulkoistamista voidaan pitää organisaation rakenteen muutoksena, jolloin myös tietoturvaa koskevien osien tulisi muuttua ulkoistusta tehdessä. Tietoturvapolitiikan ohjeistukset tulisi päivittää koskemaan uutta organisaatiorakennetta, josta voi seurata uusia vaatimuksia ulkoistetuille liiketoimille. Lisäksi, jos tietoturvaa koskevia asioita käsitellään yhdessä IT-osaton kanssa, tietoturvaa koskevia päätöksiä ei välttämättä voida käsitellä yhtä tehokkaasti kuin, jos tietoturvatiimi toimisi omana yksikkönään. Matriisiorganisaatioiden tiedonkulku on huomattavasti monimutkaisempaa kuin hierarkkisessa organisaatiossa, ja tämän takia myös matriisi- ja hierarkkisissa organisaatioissa tulisi ottaa kantaa rakenteisiin liittyviin tietoturva-asioihin (Dutta & McCrohan, 2002).

Kilpailuympäristö

The Computer Institute havaitsi neljä kilpailuympäristön tekijää, joilla on mahdollinen yhteys kyberhyökkäyksiin. Näitä tekijöitä ovat immateriaalioikeuksien muodostama kilpailuetu, toimialalla vallitseva muutos, alalle pääsyn esteet ja organisaation kokema kilpailu toimialalla (CSI, 2002). Esimerkiksi sellainen organisaatio, jonka kilpailukyky perustuu jatkuviin kasvupanostuksiin tutkimus- ja kehitystoimintaan, ja jolla on suuri määrä asiakkaita ja toimittajia kilpailulla markkinalla – toden-

näköisesti kohtaa suurempaa kybervaikuttamisen uhkaa kuin vakaalla toimialalla ja vakaassa kilpailuympäristössä toimiva organisaatio. Lisäksi paljon mediahuomiota saaneet organisaatiot johtuen esimerkiksi yrityskaupoista tai uusien tuotteiden lanseerauksista, ovat useammin hakkereiden kohteena. Mainittujen dynaamisten vaikuttumien takia, ainoastaan yritysjohdon sitoutuneisuus ja syventyneisyys mahdollistavat tämänkaltaisiin uhkiin varautumisen aikaperspektiivistä huolimatta (Dutta & McCrohan, 2002).

Yrityskulttuuri

Jokaiselle organisaatiolla on omat kirjoittamattomat sääntönsä ja jotkin tavat, arvot tai uskomukset voivat tuntua absurdeilta ja joita voi olla vaikea selittää ulkopuoliselle. Tämänkaltainen kulttuuriaspekti voi tehostaa tai heikentää organisaation tietoturva-asemaa. Yhdysvalloista on esimerkkejä, joissa yliopiston löyhä tietoturvasuhtautuminen opiskelijoiden tekemisiin on kostautunut kriittisten yritysten tietoturvahyökkäyksien muodossa, joissa hyökkäykset oli käynnistetty tiettyjen yliopistojen palvelimilta (Dutta & McCrohan, 2002).

Hyvään asiakaskokemukseen pyrkivä yritys voi myös aiheuttaa tietoturvariskin positiivisen yrityskulttuurin kautta. Esimerkiksi yritys, joka pyrkii hyvän asiakaskokemuksen luomiseen, voi jossain tapauksissa johtaa sensitiivisen tiedon välittämiseen ja standardiprosessien ohittamiseen. Erilaisen yrityskulttuurin muodostamien riskien havaitseminen ja niihin vastaaminen, on johdon tärkeimpiä tehtäviä (Dutta & McCrohan, 2002).

Standardoidut prosessit ja päätöksenteko

Standardoitujen prosessien ja päätöksenteon merkitys on erittäin suuri minkä tahansa organisaation kannalta, sillä ne kiteyttävät organisaation jatkuvien toimintojen ja näiden ohjaukseen liittyvän päätöksenteon yhteiseksi toiminnaksi, jolloin organisaatioiden päämäärien tavoittaminen helpottuu. Turvallisuusasiat tulee siten sitoa arkipäiväisiin rutiineihin, jotta turvallisuuteen kytkeytyvät tavoitteet voidaan yhdistää organisaation operatiiviseen toimintaan tehokkaasti ja taloudellisesti (Dutta & McCrohan, 2002).

Näitä prosesseja ovat esimerkiksi salasanojen turvallisuuteen liittyvät asiat, turvallisuusuhkista raportoiminen ja tiedottaminen sekä uhkiin vastaaminen. Luontainen tapa sisällyttää turvallisuuteen kytkeytyviä asioita päivittäisiin työtehtäviin auttaa organisaatiota pysymään ajan tasalla mahdollisista

uhista sekä turvaamaan oman toimintansa jatkuvalla valvonnalla ja seurannalla (Dutta & McCrohan, 2002).

Koulutus, harjoittelu & tietoisuus

Aktiivinen henkilöstön koulutus ja harjoittelu auttavat lisäämään heidän tietoisuutta turvallisuudesta, ja samalla prosessien turvallisuusuhkien havaitseminen tehostuu. Koulutuksen tulisi painottaa organisaation omaisuuden turvaamista, ja mitä erilaisia skenaarioita voi seurata, jos näitä periaatteita ei noudateta. Nämä seuraukset voivat olla välittömiä yksilön kannalta, jos sääntöjä ei noudateta. Suuremmat vaikutukset kokee kuitenkin organisaatio, ja se millä tavalla henkilöstön toimet vaikuttavat organisaation omaisuuteen ja raskaasta tilanteesta selviämiseen (Dutta & McCrohan, 2002).

Dutta & McCrohan (2002) ehdottavat, että organisaation tulisi järjestää tietoturvaharjoituksia tiedottaakseen henkilöstöä tietyistä toimista, joita tulisi harjoittaa turvallisuutta uhkaavissa tilanteissa. Turvallisuuskoulutuksen tulisi myös kattaa tavanomaisten teknologisten ratkaisujen välineet kyberturvariskien vähentämisessä. Dietrichin ym. (2004) mukaan tietoturvaharjoituksia tulisi järjestää yleisten paloturvallisuusharjoitusten lisäksi, sillä näillä harjoituksilla on todettu olevan organisaation tavoitteiden kannalta tehostava vaikutus.

Kyberturvaan liittyvät harjoitukset voidaan jakaa kolmeen tapaan (Dietrich, ym. 2004):

1) Henkilöstön tietoisuuden lisääminen kyberturvan suhteen: opetus on luentopohjaista.
2) Harjoitus toteutetaan oppimisen näkökulmasta: henkilöstö oppii tiettyjen prosessien kautta tietoturvan ilmentymistä. Henkilöstölle kuvataan, miten missäkin tilanteessa tulisi toimia.
3) Harjoitus voidaan toteuttaa testimielessä ja testata henkilöstön todellista valmiutta havaita ja torjua hyökkäyksiä: tällöin kuvataan mahdollisimman totuudenmukainen tilanne, jossa organisaation kohtaa kuvitellun, mutta konkreettisen uhan.

Turvallisuuden eteen tulee tehdä ponnisteluja organisaation jokaisella tasolla varsinkin ylimmän johdon osalta, jonka vastuulla on rakentaa organisaatiolle tarkoituksenmukaiset puitteet suunnittelulle ja resurssien kohdentamisjärjestelmälle tavoitellun turvallisuustason takaamiseksi (Dutta & McCrohan, 2002).

Tietoturvaharjoituksen toteuttaminen

Toimiva johto	IT-osasto	Hallitus
- Toimeenpanee aloitteen, hakee hyväksynnän hallitukselta. - Vuoropuhelu IT-osaston suuntaan koko harjoituksen ajan.	- IT-osasto tekee aloitteen, toimiva johto voi osallistua. - Vuoropuhelu toimivan johdon suuntaan.	- Hyväksyy/hylkää aloitteen.
1. Määrittele ulottuvuus		
- Testaanko esimerkiksi yksittäisen liiketoimintayksikön vai koko organisaation valmiutta vastata tietoturvauhkaan?		
2. Määrittele testattavat konseptit		
- Onko tavoitteena harjoitella uhkien havaitsemista, torjumista vai molempia? Onko harjoituksen tarkoituksena selvittää henkilöstön yleistä tietoturvaymmärrystä? Kauanko harjoituksen olisi tarkoitus kestää?		
3. Valitse toteutustiimi		
- Ulkopuolinen kyberturvayhtiö yleensä valitaan toteuttajaksi. - IT-osastosta alistetaan muutama työntekijä toteutustiimille. Tiimiin koko riippuu organisaation koosta. - Yleensä harjoitukseen ottaa osaa myös sellaiset funktiot, jotka eivät ole suorassa yhteydessä kyberturvallisuuteen, kuten HR- ja viestintäosasto.		
4. Kehitä todenmukainen taustatarina		
- Lisää kuvitteellisia tapahtumia, jotka täydentävät harjoitusta. ”Luovuus on tärkeää, mutta realismi välttämätöntä.”		
5. Toteuta harjoitus		
- Harjoitukset käynnistyvät ”pelinjohtajan” aloitteesta, kun hän antaa ensimmäisen tilannekuvan organisaatiolle. Harjoitus jatkuu uusien tilanteiden ja toteutustiimin reagoinnin myötä näihin uusiin tilanteisiin.		
6. Harjoituksen jälkeinen raportointi		
- Missä määrin päästiin tavoitteisiin? Mitä organisaatiosta opittiin harjoituksen avulla? - Tärkeää on saada työntekijöiltä yksilökohtaista palautetta.		

Taulukko 1: Tietoturvaharjoituksen toteuttamiseen liittyvät vaiheet (Dietrich, ym. 2004 & Vilander, 2019).

2.4.3 Teknologia

Teknologia on organisaation kolmas kulmakivi, joka turvaa organisaation tietoturva-asemaa. Vaikka vastuualueiden osoittamat tehtävät osoittaisivat IT-osaston tai tietohallintovastaavan olevan vastuussa teknologiaa koskevista päätöksistä, ylimmän johdon vastuulla on silti ymmärtää kriittisimpien teknologisten ratkaisujen komponenteista. Heidän tulee muun muassa olla tietoisia ”Defense in

Depth”-konseptista (Power, 2000), joka sisältää turvallisuusteknologiat keskeisimmistä komponenteista. Nämä ovat: palomuurit ja tunkeutumisen havaitsevat laitteet, salasanojen turvaaminen, digitaalisten avainten salaaminen, turvallisten palvelimet ja VPN-verkot (Dutta & McCrohan, 2002). Näistä seuraavaksi enemmän.

Palomuurit ja tunkeutumisen havaitseminen

Palomuurien tehtävä on jakaa verkkoliikenne kahtia suojattuun ja suojaamattomaan osaan. Näiden laitteiden suorituskyvyn arvioinnin tulisi tasapainotella helppokäyttöisyyden, riskien vähentämisen ja kustannustehokkuuden välillä. Puolustuksen ylläpitämiseksi ei riitä ainoastaan, että organisaation tietojärjestelmiä suojelee laite, jonka ensisijaisena tehtävänä on suojata verkkoliikennettä. Tarvitaan myös sellaisia laitteita, jotka pyrkivät aktiivisesti havaitsemaan mahdollisia tunkeutujia verkkoympäristössä. Lisäksi tunkeutumisen havaitsevat laitteiden tehtäviin kuuluu myös havainnoista raportoiminen johdolle (Dutta & McCrohan, 2002).

Salasanojen monitasoinen käyttö

Tietoturvapolitiikassa tulisi antaa yleisiä suuntaviivoja organisaation toimintaan liittyen (Holopainen, ym. 2013). Tällöin esimerkiksi salasanojen vaihtamisesta ja niiden uudelleenkäytön mahdollisuuksista olisi hyvä laatia selkeät ohjeistukset. Organisaation tulisi myös erikseen luokitella sellaiset tiedot, joihin käsiksi pääsemiseen vaadittaisiin eri salasanoja. Duttan & McCrohanin (2002) mukaan salasanahierarkian luominen tiedon salaisuusasteen mukaan (erittäin salainen – julkinen) on kriittinen komponentti organisaation turvallisuustason tavoittelussa. Tällöin yksittäisen salasanan päätyminen vääriin käsiin ei vaarantaisi koko systeemiä ja näin merkitsisi pienempää vahinkoa organisaatiolle.

Salasanojen monitasoinen käyttö vaatii organisaatiolta niin teknologisia kuin hallinnollisia ja ylläpidollisia kykyjä, jotta organisaation omaisuus eri tietojen suhteen olisi turvattu. Hallinnolliset periaatteet eli aiemmin mainittu tietoturvapolitiikka pitää huolen, että ainoastaan ne tahot joiden kuuluisi päästä salaisista tiedoista osallisiksi, myös pääsevät. Lisäksi salasanojen monitasoiselle on myös se hyöty, että nämä periaatteet ovat usein kustannustehokkuuden kannalta hyvin vaikuttavia toimia organisaation tietoturvan tehostamisessa (Dutta & McCrohan, 2002).

Julkisen avaimen käyttö ja infrastruktuuri (PKI)

Julkisten avaimien infrastruktuuri koostuu hyvin monista erilaisista teknologioista, joiden pääperiaatteista johdon tulisi olla tietoinen (Dutta & McCrohan, 2002). Julkisten avaimien käyttö yleistyy samassa suhteessa, kun kryptografisten sovellusten määrä kasvaa taloudessa. **Julkisen avaimen infrastruktuuri** (public key infrastructure, PKI) on luotu salaisten tiedostojen, dokumenttien tai sovellusten lähettämiseen ja lukemiseen, jossa tiedon vastaanottaja ja tiedon lähettäjä tunnistetaan julkisen avaimen avulla. Näiden avaimien avulla voidaan myös varmistaa tiedon oikeellisuus ja varmistaa tiedon päätyminen ainoastaan tarkoitetuille vastaanottajille.

PKI:n luominen on tekninen haaste, mutta se on myös hallinnollinen haaste, sillä jotta PKI voisi toimia hyvin, se tarvitsee myös organisaation hallinnoimaan näitä julkisia avaimia. Vaikka tällä hetkellä ei yhteiskunnassa ole laajaa PKI:ta, tämän infrastruktuurin luominen helpottaisi tiedon lähettäjien ja vastaanottajien identiteettien tunnistamista sekä tiedon oikeellisuuden varmistamista. Lisäksi infrastruktuurin luominen vaatisi eri toimialojen yhteistyötä, jotta tarvittavat komponentit voitaisiin sulauttaa yhteen PKI:n luomiseksi (Dutta & McCrohan, 2002).

Palvelinten turvallisuus

Laskentateho on tuonut paljon hyvää yhteiskuntaan, mutta samalla serverien toimintakyky on kasvanut ja nykyään ne tarjoavat hyvin suuren määrän erilaisia toiminnollisuuksia. Tämä voidaan nähdä uhkana ja mahdollisuutena. Koska yritys harvemmin tarvitsee kaikkia toimintoja hoitaakseen omaa ydin liiketoimintaansa, näiden ylimääräisten toimintojen rajaaminen pois voi olla merkittävä turvallisuutta lisäävä päätös. Yritysjohdon vastuulla on päättää tarvittavista palvelinratkaisuista, jotka tyydyttävät organisaation tarpeet ilman lisätoimintoja (Dutta & McCrohan, 2002).

Rajatessaan ylimääräiset toiminnot pois, organisaatio voi välttää uusien teknologioiden tuomat haasteet, joita ei vielä palvelinratkaisuja tehdessään oltu vielä osattu ottaa huomioon. Tämänkaltainen toiminta vaatii hyvää kommunikaatiota johdon, käyttäjien ja systeemin ylläpitäjien välillä.

Virtuaalinen yksityisverkko (VPN)

Virtuaalinen yksityisverkko (virtual private network, VPN) tarjoaa yksityisen verkkoasioinnin turvallisuuden, kun käyttäjä asioi julkisen verkon yli. VPN salaa käyttäjän sijainnin esimerkiksi web-

sovelluksilta, jolloin web-sivusto ei pysty jäljittämään verkossa operoivaa VPN-käyttäjää. Tällöin esimerkiksi sijaintitiedot tai muilla sivustoilla vierailu ei paljasta käyttäjää.

VPN-yhteyden suosio perustuu mahdollisuuteen perustaa tilapäisverkko riippumatta käyttäjän ympäristöstä tai sijainnista. Käyttäjä voi lähettää ja vastaanottaa tiedostoja verkon yli, ilman että ulkopuolinen taho pystyisi purkaa käyttäjän verkkoliikenteen ymmärrettävään muotoon. Viestintää harjoitetaan hyvin erilaisista lähtökohdista, jolloin myös turvallisuusperiaatteiden pohjalta VPN tarjoaa turvallisen sensitiivisen tiedon lähettämistä ja vastaanottamista tarjoavan teknologisen ratkaisun (Dutta & McCrohan, 2002)

Loppujen lopuksi voisi sanoa, että teknologian puolella on monia komponentteja, joiden arviointia yritysjohdon tulisi tehdä asettamiensa tietoturvallisuuteen liittyvien tavoitteiden saavuttamiseksi. Pätevän IT-osaston palkkaaminen voi olla vastaus parempaan teknologiseen varautumiseen ulkoisia uhkia vastaan, mutta se ei riitä jos yritysjohto ei ole itse tietoinen kriittisimpien teknologisten komponenttien vaikutuksesta organisaatioon. IT-funktion ja johdon välinen vuorovaikutus tulisi olla jatkuvaa, jotta molemmilla osapuolilla olisi käsitys organisaation kyvyistä ja mahdollisuuksista sekä tavoitteista ja nykytilasta. Tavoitteiden ja suoriutumisen tasoa johto voi mitata IT-osaston kanssa käydyn vuoropuhelun avulla. Saatujen tietojen avulla johto voi tehdä kustannus-/hyötyarviointia parempien päätösten tueksi (Dutta & McCrohan, 2002).

Ylimmän johdon rooli on tärkeä tunnistaa kriittisimmät teknologiat strategian suhteen, sillä ei ole olemassa täydellistä kyberturvaa digitaalisessa nykymaailmassa. Ajan kanssa tulee muuttua ja on vain viitteitä siitä, millaisia hyötyjä mikäkin teknologinen investointi voi organisaatiolle tuoda. Ja tästä syystä johto on parhaassa asemassa tehdäkseen holistisesti parempia päätöksiä teknologian suhteen eikä päätöksentekoa voi sen takia luovuttaa IT-osastolle sellaisenaan (Dutta & McCrohan, 2002).

2.4.4 Ylin johto

Kyberturvallisuuden määrittäminen on monitasoinen ja kompleksi, sillä siinä tulee ottaa huomioon kolme eri näkökulmaa: kriittinen infrastruktuuri, organisaation rakenne sekä teknologiset päätökset. Johto pyrkii näiden kolmen rakennuspalikan arvioinnin perusteella jakamaan resursseja tehokkaasti. Resurssien tehokkaaseen jakamiseen johto tarvitsee tunnistaa organisaation omaisuus, arvioida näihin omaisuuden eriin liittyviä riskejä sekä pyrkii asettamaan liiketoiminnalle ympäristöä koskevia kontrolleja (Dutta & McCrohan, 2002). Näistä tarkemmin seuraavaksi.

Omaisuuden tunnistaminen

Omaisuuden tunnistamisprosessi auttaa käyttäjiä, ylläpitäjiä ja ylintä johtoa ymmärtämään organisaation kriittisimmän omaisuuden, joka koskee systeemeissä kulkevaa tietoa. Jotta tietoa voitaisiin luokitella, on tietoja tarkasteltava kolmen kriteerin avulla: tiedon salassapidettävyys, tiedon oikeellisuus ja tiedon saatavuus. Kaikki tieto ei siten ole organisaation näkökulmasta kriittistä, sillä jos jokin näistä kriteerin tasoista on alhainen, kyseinen tieto ei todennäköisesti ole yhtä arvokasta kuin päinvastaisessa tilanteessa. Tiedon arvokkuuden kannalta tulisi siten arvioida sen vaikutusta organisaation jatkuvuuteen (Dutta & McCrohan, 2002).

Jos esimerkiksi organisaatio luokittelisi sen asiakkaita koskevat tiedot niin salassapidettävyyden, oikeellisuuden kuin tiedon saatavuutta koskevat vaatimukset korkeiksi, kun taas toimittajia koskevien tietojen luokitteluaste olisi pykälän matalampi kaikissa näissä kategorioissa. Tällöin turvallisuusjärjestelmien tulisi pystyä mukautumaan asiakkaan tietoja enemmän varjeleviksi ja turvallisemmiksi verrattuna toimittajien vastaaviin tietoihin (Dutta & McCrohan, 2002).

Riskien arviointi

Riskiarvioinnissa tulisi aina lähteä siitä, miten todennäköisenä voidaan pitää jonkin tapahtuman tapahtumista. Todennäköisyyksien arvioinnin lisäksi näitä tapahtumia koskevat kustannukset tulisi myös pystyä määrittämään, koska vain tällöin organisaatio voi määrittää sitä uhkaavien toimijoiden vaikutukset. Näistä syistä tarvitaan riskiarviointia (Dutta & McCrohan, 2002).

Turvallisuutta uhkaavia toimintoja on kolmenlaisia: tiedon varastaminen, tiedon väärinkäyttö ja kyvyttömyys tarjota sidosryhmille näiden tarvitsemia palveluita sovittuna aikana. Aiemmin käsiteltyihin kriittiseen infrastruktuuriin, organisaatioon sekä teknologiaan liittyviä riskikomponentteja tulisi voida pienentää yleisesti, sillä jos teknologiaan liittyvä riski pienenee, se ei vielä tarkoita organisaation kokonaisriskin pienenemistä. Rakenteisiin liittyvä tiedon väärinkäytön riski ei teknologisen kehityksen kautta pienene, vaan siihen tulee vaikuttaa organisaatio-kappaleessa esiteltyjen tekijöiden avulla (Dutta & McCrohan, 2002).

Uhkien ilmaantuvuus johtuu siis niiden osatekijöistä. Organisaatioon voi jäädä riskitekijöitä, jos esimerkiksi henkilökunnan taustoja ei tarkasteta kunnolla tai henkilöstölle ei järjestetä tietohallintoon liittyviä koulutuksia, jolloin riskitekijöiden vaikutus voi pidemmässä juoksussa aiheuttaa riskien

konkretisoitumista. Jokaisella kolmella komponentilla on erilainen riski-ilmentymä, johon johdon tulisi ottaa kantaa, ja lisäksi nämä komponentit tulisi tunnistaa ja arvioida erikseen (Dutta & McCrohan, 2002).

Uhat syntyvät myös muista lähteistä kuin pelkästään ihmisen aiheuttamista toimista ja nämä uhkatoimijat voivat vaikuttaa hyvin erilaisin tavoin. Tästä esimerkkinä on luonnonilmiöiden aiheuttamat häiriöt kriittiselle infrastruktuurille. Tulipalot, tulvat, maanjäristykset ja muut luonnon mullistukset ovat aiheuttaneet enemmän haittaa kriittiselle infrastruktuurille kuin terroristit heidän olemassa olon aikana. Organisaatioon sisäiseen toimintaan liittyvät uhat voivat taas syntyä henkilöstön tyytymättömyydestä tai esimerkiksi kilpailijan yrittäessä hyödyntää organisaation heikkoihin rakenteisiin liittyviä asioita (Dutta & McCrohan, 2002).

Teknologiset haasteet syntyvät laitteistojen ja ohjelmistojen yhteistoiminnan seurauksena, jolloin riskit voivat konkretisoitua. Teknologiaan, kriittisen infrastruktuuriin ja organisaatiota koskevaan arvioon tulisi sitouttaa ihmisiä niin käyttäjistä, ylimmästä johdosta, IT-puolelta, ja julkiselta puolelta parhaimman objektiivisen näkökulman luomiseksi (Dutta & McCrohan, 2002).

Toimintaympäristön kontrollointi: yleiset ja sovelluksiin liittyvät kontrollit

Erilaisten kontrollien asettaminen lähtee turvallisuuspolitiikasta, jossa mainitaan yleiskielellä ne periaatteet, joita organisaatio on sitoutunut noudattamaan. Toimintaympäristölle asetettujen kontrollien päätehtävänä on sitten kääntää nämä yleiskielenohjeistukset toteuttamiskelpoiselle kielelle koskemaan konkreettisia organisaation prosesseja. Kontrolliympäristö voidaan jakaa kahteen: yleisiin IT-kontrolleihin ja sovelluksia koskeviin kontrolleihin. Lisäksi nämä toimintaympäristön komponentit voidaan vielä jakaa pienempiin osatekijöihin. Yleisiin kontrolleihin kuuluu kaikki IT-funktioihin liittyvät asiat, joita ovat: fyysiset, tiedon sisältöön, toimeenpanoon, toimintoihin ja hallinnollisiin kontrolleihin liittyvät kontrollit. Sovelluspohjaisiin kontrollit koskevat ainoastaan tiettyjä systeemejä ja sovelluksia (Dutta & McCrohan, 2002).

Fyysiset kontrollit: koskevat laitteistoa, ohjelmistoja, käytettyä verkkoa sekä fyysisiä toimitiloja. Haasteena fyysisen kontrollien tekemiselle on usein se, etteivät organisaatiot pidä kirjaa omien laitteiden käytöstä, esimerkiksi mihin tehtäviin tiettyä laitteistoa käytetään tai kuka näitä laitteistoja käyttää sekä mikä hänen valtuutuksen tasonsa on. Riskien havaitseminen niin vaarallisten työyhdistelmien kuin muiden riskien suhteen vaikeutuu, jos organisaatio ei pidä kirjaa laitteistojen ja ohjelmis-

tojen käyttöön liittyvistä asioista. Tähän liittyviä resurssien käyttöä tehostavia ohjelmistoja on tarjolla, mutta niiden käyttöönottoon liittyy usein paljon organisaation resurssien käyttöä, kuten johdon aikaa. Lisäksi käyttöönottoon liittyvä aika on yleisesti pois yrityksen tuotannosta. Näihin syihin vedoten, organisaatio voi perustella nykyisten prosessien toimivan kohtuullisen hyvin, jolloin riskien havaitsemiseen ei käytetä lisää resursseja (Dutta & McCrohan, 2002).

Laskentatehon halpenemisen ansiosta organisaatio on voinut hankkia yhä uusia prosesseja tehostavia laitteistoja ja ohjelmistoja, joiden valvominen muuttuu yhä haasteellisemmaksi, jos näihin hankintoihin liittyvää resurssien valvontaan liittyvää järjestelmää ei ole. Esimerkki fyysisen kontrollin puutteesta on kannettavan tietokoneen häviäminen tai datakeskuksen sijoittaminen toimitilan kellarikerrokseen tulva-alueella (Dutta & McCrohan, 2002). Lisäksi on olemassa myös muita fyysisiä kontrolleja, joita on esitelty Liitteessä 1 (Rousku, 2014).

Sisältöön liittyvät kontrollit: sisältöön liittyvien kontrollien tekeminen on paljon tärkeämpää kuin fyysisiin laitteistoihin ja ohjelmistoihin liittyvät tarkastukset, ja siksi tiedon tunnistaminen ja luokittelu on tulisi olla organisaation tärkein valvonnan kohde ympäristön kontrolleihin liittyen. Sisällön tunnistamisessa lähtökohtana on tunnistaa tietojen luokat (salainen – julkinen), käyttäjät, millaisia valtuutuksia käyttäjillä on, ja mikä on käyttäjien työtehtävä käytettävän tiedon suhteen. Sisältöön liittyen kontrollien määrittely kumpuaa niin yrityksen tekemästä turvallisuuspolitiikasta, lainsäädännöstä ja yleisistä liiketoimintakäytännöistä (Dutta & McCrohan, 2002).

Toimeenpanoon liittyvät kontrollit: tietojärjestelmän kehitykseen liittyy järjestelmän kehitystyö sekä testaus, joiden tekeminen tulisi eriyttää eri osastojen tehtäväksi. Tällöin vältetään eturistiriitojen syntyminen oman työn tarkistamisen suhteen. Lisäksi motivointi ja vastuunjakaminen on parempi eriytetyssä mallissa (Dutta & McCrohan, 2002).

Jatkuviin toimintoihin liittyvät kontrollit: jatkuviin toimintoihin liittyvät kontrollit pyrkivät vähentämään laitteistoihin, ohjelmistoihin, sisältöön sekä tietoverkkojen kautta mahdollista järjestelmän vaarantamista vahingossa tai suunnitteluvirheen takia. Lokien, automaattisten virusturvapäivitysten ja varajärjestelmien käyttäminen ovat esimerkkejä jatkuvien toimintojen valvonnasta (Dutta & McCrohan, 2002).

Hallinnolliset kontrollit: hallinnolliset kontrollit pyrkivät mukauttamaan prosesseja, henkilökuntaa ja organisaatiorakennetta ilmaistun turvallisuusaseman mukaiseksi. Tähän voidaan pyrkiä esimerkiksi järjestelmällä tietojärjestelmien turvallisuusharjoituksia ja kouluttamalla henkilöstölle turvallisuutta koskevien laitteistojen ja ohjelmistojen suhteen (Dutta & McCrohan, 2002).

Liiketoimintojen lokeroiminen omiksi selkeiksi vastuualueiksi voi auttaa turvallisuusaseman tavoittelussa, mutta esimerkiksi matriisiorganisaatioissa tietojen vaihtaminen organisaation eri tasojen ja liiketoimien välillä on toiminnan perusedellytys. Matriisiorganisaation suhteen voisin perustella, ettei hallinnollisten kontrollien asettaminen auta riskien havaitsemisessa, mutta jo kontrollien olemassaolo vaikuttaa itsessään henkilöstön suhtautumiseen tietojen turvallisuudesta. Esimerkiksi valtuutuksien lopettaminen heti työsuhteen päätyttyä, on yksi mahdollinen tapa ilmaista hallinnollisia kontrolleja (Dutta & McCrohan, 2002).

Sovelluksiin liittyvät kontrollit: sovelluksia koskevat kontrollit koskevat ainoastaan tiettyjä systeemejä tai sovelluskomponentteja. Esimerkiksi yrityksen sisäisessä viestinnässä käytetty Intranet tulisi olla vain henkilöstöön kuuluvien ihmisten käytössä. Lisäksi laitteistojen ja ohjelmistoihin liittyvät varmistukset yleensä kuuluvat palomuurien ja uhkien havaitsemislaitteiden vastuulle. Sovelluksiin liittyvä kontrolli voi myös olla esimerkiksi sähköpostiliitteen koon rajoittaminen tai henkilöstön tietokannan manipuloimisen estäminen palkkojen suhteen. Ylläpitäjän vastuulla on asettaa sovelluksille tarvittavat kontrollit (Dutta & McCrohan, 2002).

2.5 Kyberturvallisuus sisäisen tarkastuksen näkökulmasta

Sisäinen tarkastus lähestyy tietoturvakysymyksiä ISO 27001-standardin kautta. Tässä tutkimuksessa käyty keskustelu lähtee ISO 27001-standardin asettamasta kehyksestä, mutta ei ota kantaa itse standardiin. Tietoturva-asiat ja laajemmin kyberturvallisuuden käsittely lähtee siitä oletuksesta, että organisaatiot pyrkivät omassa sisäisessä tarkastuksessaan noudattamaan ISO 27001-standardin asettamia vaatimuksia.

Haastatteluissa läpikäydyt aiheet koskettavat ISO 27001-standardia, mutta itse standardista ei keskustella, sillä siitä keskusteleminen olisi triviaali valinta eikä välttämättä toisi keskustelua riittävän abstraktille ja geneeriselle tasolle. Tällöin ei voisi esimerkiksi kysyä, miten organisaatiot toimivat kyberturvan suhteen yleisesti. Keskustelu jäisi tässä mielessä liian alhaiselle tasolle, ja lopputuloksena saataisiin korkeintaan suosituksia yksittäisten organisaatioiden toimintaan kyberturvallisuuden suhteen, mikä ei ole tämän tutkimuksen päätavoite. Päätavoitteena on selvittää: 1) kuka on tilivelvollinen ja kuka on vastuussa oleva organisaation tietoturva-asioissa; ja 2) miten hallitus ja johtoryhmä ymmärtävät organisaation kyberturvallisuuden.

3 Metodit & Data

3.1 Metodit

Kuvaileva tapaustutkimus

Scapensin (1990) mukaan kuvailevat tapaustutkimukset pyrkivät kuvaamaan laskentajärjestelmiä, tekniikoita ja liiketoimissa käytettyjä käytännön menetelmiä. Haastateltavat organisaatiot valitaan niin, että tutkimuksen avulla voitaisiin kuvata jotakin ilmiötä mahdollisimman todenmukaisesti näiden organisaatioiden eroavaisuuksien/samankaltaisuuksien avulla. Lopputuloksena syntyy kuvaus tutkimuksen kohteena olevasta laskentatoimen käytännön ilmiöstä.

Tutkiva tapaustutkimus

Scapensin (1990) mukaan tutkivaa tapaustutkimusta voidaan käyttää apuna tutkittaessa erilaisia laskentatoimen käytäntöjä eri organisaatioissa. Näiden tapaustutkimusten tavoitteena on esittää ennakoiva ja valmistelava hypoteesi sellaisille tutkimuksille, jotka tutkisivat tutkivan tapaustutkimuksen aikana kehiteltyä hypoteesia jonkin uuden teorian perustaksi laskentatoimen kehyksessä. Tutkiva tapaustutkimus on tällaisen projektin ensimmäinen askel.

Valittu tutkimusmenetelmä

Ensisijaiseksi tutkimusmenetelmäksi valittiin kuvaileva tapaustutkimus, sillä tutkimuskysymyksien luonne viittaa tähän tutkimusmenetelmään. Lisäksi tutkimuksen ensisijaisena tavoitteena oli mennä tapaamaan eri alojen ja positioiden edustajia, ja selvittää miten kyberturvallisuusvastuut heidän mielestään jakautuvat. Tutkimuksella ei täten pyritä etsimään mitään uutta teoriaa, vaan tutkitaan kyberturvallisuusilmiötä yleisesti. Jos tutkimus onnistuu noudattaa hyviä akateemisia käytäntöjä, tuloksena voi olla pieni näyte siitä, miten kyberturvallisuusvastuut ja siihen liittyvät asiat organisaatioissa ymmärretään yleisesti.

Tutkimus on ainutlaatuinen siinä haastateltujen ihmisten takia, ja näitä samoja kysymyksiä voisi esittää myös muille tietojärjestelmistä perillä oleville ihmisille ja saatu tulos voisi olla samankaltainen

(tai erilainen) kuin tässä tutkimuksessa. Tästä syystä voisi sanoa, että tutkimuksella on tutkivan tapaustutkimuksen piirteitä, vaikka tutkimuksen ensisijaisena tarkoituksena ei olekaan luoda hypoteesia uuden teorian kehittämistä varten. Saatua tutkimustulosta voidaan toki jossain määrin käyttää tätä tarkoitusta varten, ja tästä syystä voisi sanoa tämän tutkimuksen sisältävän piirteitä kahdesta tutkimusmenetelmästä.

3.2 Data

Datan kerääminen & käsittely

Data keräämisessä käytettiin yksilöhaastatteluita, ja jokainen haastattelu nauhoitettiin datan pysyvyyden ja tutkimuksen tarkkuuden varmistamiseksi. Haastateltavat löydettiin erään haastateltavan kautta, joka suositteli useampaa asiantuntijaa konsulteista talousjohtajiin ja systeemiarkkitehteihin. Lopulliset haastateltavat valittiin satunnaisesti näiden joukosta sen perusteella, ketkä olivat helpointen saatavilla haastatteluiden toteutusvaiheessa.

Datan käsittelyssä käytettiin avuksi Google Docsin tarjoamaa puhekirjoitus-sovellusta, jolloin tekstintunnistaminen jätettiin jossain määrin teknologian vastuulle, vaikka samalla tutkija valvoikin sovelluksen ehdottamia virkkeitä ja lauseita. Lisäksi haastatteluiden äänityksien avulla tutkijalla oli mahdollisuus palata haastatteluihin uudestaan ja tehdä tarkennuksia, jos esimerkiksi tietty asiayhteys ei selvinnyt jälkikäteen vastauksista. Teknologian ja mekaanisen työn yhdistelmä tuotti todennäköisesti parhaan mahdollisen lopputuloksen datan käsittelyn suhteen.

Tutkimuksen laajuus & syvyys

Tutkimuksessa on haastateltu kuuden eri organisaation edustajia erilaisilla positioilla: tutkimukseen otti osaa kaksi talousjohtajaa, operatiivinen johtaja sekä kaksi IT-alan neuvonantajaa ja yksi tietoturva-asiantuntija. Lisäksi nämä organisaatiot, joiden edustajia haastateltiin, toimivat hyvin erilaisilla aloilla: organisaatiot, joita haastateltiin toimivat rakennus-, lakimies- ja konsulttialalla sekä valmistavalla teollisuuden alalla. Valintaa voidaan perustella valitun tutkimusmenetelmän avulla, sillä tutkittua ilmiötä pyritään ymmärtää organisaatioiden eroavaisuuksia/samankaltaisuuksia tutkimalla. Tä-

män lisäksi, erilaisten organisaatioiden ja erilaisissa positiossa toimivien ihmisten haastattelulla saadaan todennäköisesti paras mahdollinen lopputulos erilaisten henkilöhistorioiden ja kokemuksien takia. Haastateltavat on esitelty liitteessä neljä.

Haastattelukysymykset luotiin Dutta'n & McCrohan'n (2002) tutkimusaiheiden pohjalta, joita on avattu tässä tutkimuksessa luvusta 2.4 alkaen. Neuvoa pyydettiin tutkimuskysymysten suunnittelussa ulkopuoliselta taholta, joka on hyvin merkittävässä roolissa tämän tutkimuksen toteuttamisen kannalta. Lopulliset haastattelukysymykset on pyritty luomaan mahdollisimman neutraaleiksi ilman johdattelevaa sanamuotoa. Neutraaleilla sanavalinnoilla varmistetaan tutkimuksen puolueettomuutta ja vähennetään mahdollisuutta, että haastateltavien vastauksia olisi voitu johdattaa johonkin haluttuun suuntaan. Liitteestä kolme löytyvät nämä nimenomaiset haastattelukysymykset, joita tutkimuksessa on käytetty.

3.2.1 Reliabiliteetti

Tutkijan takia vaarantuva reliabiliteetti

Tutkijan aiheuttamia vaikutuksia on kuvattu reaktiivisiksi vaikutuksiksi, joita syntyy tutkijan läsnäolosta. Tällöin haastateltava ei voi käyttäytyä neutraalisti, vaan haastateltavan sanomia asioita voidaan pitää jossain määrin virheellisinä (McCall & Simmons, 1969). Tällöin haastateltavan sanomisia ei voida pitää reliabiliteetin näkökulmasta uskottavina, ja koko tutkimustulos voi antaa väärän kuvan tutkitusta ilmiöstä. McKinnon'n (1998) mukaan, jos haastateltava kokee tutkijan olevan esimerkiksi ylimmän johdon "vakooja", voidaan edellä kuvatun mukaista neutraalista poikkeavaa asennoitumista pitää uhkana tutkimuksen reliabiliteetille.

Tässä tutkimuksessa tutkijan takia vaarantuvaa reliabiliteettia voidaan puolustaa sillä, ettei haastateltavat todennäköisesti kokeneet omaa asemaansa uhatuksi tutkijan taholta. Tämä johtuu siitä, että kaikki haastateltavat olivat ulkopuolisia, eikä heitä kohtaan ollut minkäänlaisia eturistiriitoja suuntaan tai toiseen.

Tutkijan tekemät virhearviot

Tutkijan virhearvioita voidaan kuvata Simon'n & Burstein'n (1985) mukaan "taipumuksena havainnoida jotakin ilmiötä muuten kuin 'totena' jollain johdonmukaisella tavalla". Yleensä tämä liittyy

tutkijan aistihavaintoihin siitä, miten hän tulkitsee haastateltavien vastauksia ja esimerkiksi kehonkieltä haastatteluiden aikana. Schwartz & Schwartz (1955) totesivat, että tutkija voi tehdä virhearvioita kolmessa eri vaiheessa ja nämä ovat: kirjausvaihe, tulkintavaihe ja raportointivaihe.

Jokaisen haastattelun kirjausvaihe toteutettiin äänittämällä kaikkien haastateltavien vastaukset, jolloin äänitteiden avulla tutkija pystyi jälkikäteen tarkistaa vastaukset yksittäisiin kysymyksiin. Tällöin haastattelu voitiin toteuttaa niin, että tutkijan ei tarvinnut tulkita vastauksia haastattelun aikana, vaan vasta myöhemmin. Tietysti tämä vähentää kehonkielen tulkinnallisia mahdollisuuksia ja voidaan todeta, että ainoastaan äänitteisiin nojaaminen voi vaarantaa jossain määrin tutkimuksen reliabiliteettia.

Raportointivaihe toteutettiin haastatteludatan keräämisen jälkeen niin, että jokaisen kysymyksen alle kerättiin ensin joko haastateltujen vastaukset suorina lainauksina tai referoiden vastauksien pääkohtia. Tämän jälkeen vastaukset kirjoitettiin auki samankaltaisuuksia ja erimielisyyksiä etsien. Mahdollisena voidaan pitää myös sitä, että raportointivaiheessa on kerrottu esimerkkejä, miten tietty haastateltava tietyn kysymyksen ymmärtää. Lopullinen tuloksien raportointi-osio koostuu suurimmalta osin haastateltavien suorista vastauksista ja referaateista, minkä takia voidaan todeta, ettei reliabiliteetti ole näiltä osin vaarantunut. Alla esimerkki yhden haastateltavan vastauksesta ensimmäiseen kysymykseen, josta on poistettu identiteetin mahdollistama tunnistaminen:

Kysymys 1: Mikä on kriittistä infrastruktuuria? Miten kuvailisit?

1:

- Viestintävälineet, puhelinverkko, tietoliikenneverkko.
- Ulkopuolinen palveluntarjoaja tarjoaa serveritilaa. Nämä ulkoiset palveluntarjoajat tarjoavat sovelluksia. Ulkopuoliset palveluntarjoajat myös pitävät huolen siitä, että dataan päästään käsiksi. Näille on siten vyörytetty vastuu.

3.2.2 Validiteetti

Tutkimuksen validiteetti pyrkii selittämään, miten *hyvin* saadut tulokset vastaavat tutkimuskysymykseen. Tärkeä kysymys on myös selvittää, miten hyvin tutkimuksessa haastateltujen sanomaan voi luottaa ja antoivatko haastateltavat ”totuudenmukaisimman” totuuden kuin heidän olisi ollut mahdollista antaa. Tutustutaan näihin seuraavaksi.

Tutkimuskysymys ”Kenen vastuulla organisaation tietoturvakysymykset ovat?” pyrkii selvittämään, miten organisaation eri tahojen vastuut jakautuvat, ja kuka on loppupeleissä vastuussa, jos organisaation tietoturva vaarantuu. Suomen kielessä ei ole erotettu sanaa kuvaamaan vastuussa olevaa (accountable) ja vastuullisena olevaa (responsible) niin kuin englannin kielessä. Asian merkityksellisyyttä kuvaa se, että haastatteluiden aikana eri rooleissa toimivat ihmiset antoivat erilaisia vastuumäärittelyitä ylimmälle johdolle ja IT-johdolle. Haastateltavan roolista riippuva vastuumäärittely todellisuudessa parantaa validiteettia ja tekee tutkimustuloksista uskottavampia, sillä nämä eroavaisuudet voidaan perustella uskottavasti accountability/responsibility-käsitteillä. Tästä aiheesta on kirjoitettu lisää **Keskustelu**-osiossa (5.kappale) alkaen.

Tutkimusaiheena tietoturvakysymykset ovat lähellä reaalimaailmaa ja tällöin käytännönläheisyys korostuu. Voidaan todeta, että ulkopuolelta saatu apu niin haastattelukysymysten suunnittelun kuin haastateltavien kontaktoinnin suhteen, oli korvaamatonta. Tutkijan oma osaaminen ei todennäköisesti olisi riittänyt parhaiden mahdollisten haastateltavien seulonnassa, siitä syystä ulkopuolinen apu on hyvin perusteltavissa. On mahdollista todeta, että tutkimuksen validiteetti parani, koska eräs näistä haastateltavista auttoi oman käytännönosaamisen kautta valitsemaan sopivia haastatteluehdokkaita. Hän pääsi vaikuttamaan, mutta ei valitsemaan haastateltavia, ja jotka lopulta valittiin satunnaisotannalla. Näistä edellä mainituista syistä voidaan todeta, että haastateltavien etsintä- ja valintaprosessi paransivat tutkimuksen validiteettia.

Tutkimustuloksena saatua ”totuudenmukaisinta” totuutta voidaan puolustaa otantamäärällä, sillä vaikka joku haastateltavista olisi antanut väärän totuuden tietyn kysymyksen suhteen, tämä väärä totuus olisi voitu huomata muiden haastateltavien lausunnoista. Tämä ei tietenkään poissulje mahdollisuutta, että kaikki haastateltavat olisivat antaneet väärän totuuden yksittäiseen kysymykseen, mutta sitä voidaan pitää varsin epätodennäköisenä tutkimuksessa käytettyjen kysymysten suuri määrä huomioiden. Lisäksi haastateltavat eivät todennäköisesti ole tienneet muiden haastateltavien henkilöllisyyksiä, minkä takia he eivät ole voineet vaikuttaa toistensa antamiin vastauksiin. Haastateltavat eivät myöskään saaneet tutustua kysymyksiin etukäteen, mikä asettaa haastateltavat samaan oikeudenmukaiseen asemaan, yhtä tapausta lukuun ottamatta. Näistä edellä mainituista syistä seuraavassa pääluvussa raportoituja tuloksia voidaan pitää valideina.

3.3 Tutkimuksen puolueettomuus

Tutkijat saattavat jäädä Yinin (1984) mukaan positiivisen metodologian ”vangiksi yrittäessään valita ’edustavia’ haastateltavia”. Jos tutkijat pyrkivät löytämään jonkin uuden teorian tutkimuksillaan, he voivat omilla tutkimuskohdevalinnoillaan myötävaikuttaa halutun tuloksen saamiseen, jolloin tutkimuksen puolueettomuus voi vaarantua.

Tässä tutkimuksessa yrityksiä ei valittu tutkijan näkökulmasta tarkasti harkiten, vaan tutkittavat organisaatiot lopulta löytyivät yhden haastateltavan yhteystiedoista. Tietenkään ei voi sanoa varmasti, että olisiko tutkimuksen puolueettomuus voinut vaarantua tämän yhden haastateltavan yhteystietojen takia. Haastateltavat kuitenkin valittiin satunnaisesti tämän yhteyshenkilön monista eri vaihtoehdoista ja tästä syystä voidaan todeta, ettei tämä yhteystietojen tarjoaja vaarantanut tutkimuksen puolueettomuutta. Lisäksi tutkija vakuuttaa, ettei tutkijan omat preferenssit vaikuta tutkimukseen valittujen haastateltavien kautta.

3.4 Tutkimuksen pääjaottelun puolustaminen – onko heuristinen lähestyminen ja tutkijan oma intuitio hyvä tapa tehdä tieteellistä tutkimusta?

Tutkimuksen pääjaottelulla tarkoitetaan kriittistä infrastruktuuria, organisaatiota, teknologiaa ja ylintä johtoa. Näitä aiheita on käsitelty kappaleessa 2.4, ja joita tullaan käsittelemään seuraavassa pääluvussa **Tutkimustulosten raportointi.** Tämän pääjaottelun taustalla on tutkijan tekemä valinta oman intuition perusteella, jossa mahdollisia tutkimusasetelmia etsittiin ensin tieteellisestä materiaalista, jonka jälkeen pyrittiin valitsemaan paras saatavilla oleva tapa luoda viitekehys, jossa käsiteltäisiin yritysjohdon vastuuta yrityksen kyberturva-asioissa. Dutta & McCrohan (2002) tarjosivat tässä mielessä parhaan vaihtoehdon tutkia kahden hyvin erilaisen maailman yhteensovittamista.

Intuitio teoreettisesta näkökulmasta

Kahneman ym. (2009) jakavat intuition päätöksenteossa kahteen kategoriaan: heuristiseen ja puolueelliseen (HP) ja naturalistiseen päätöksentekoon (NPT). Näistä jälkimmäinen kehittyy toistojen myötä paremmaksi, kun esimerkiksi shakinpelaaja oppii tunnistamaan erilaisia kaavoja shakkilau-

dalta, ja jolloin hän pystyy suunnitella seuraavat siirrot luottaen enemmän omaan intuitioon kuin johonkin kuvitteelliseen statistiseen faktaan. Kahneman ym. (2009) sanovat myös ”hiljaisen tietämyksen” selittävän paljon sellaista päätöksentekoa, johon sisältyy paljon tietoa.

Heuristinen ja puolueellinen näkökulma perustuu ajatukselle, että joku sellainen päätös, joka voidaan jakaa faktisesti moniin erilaisiin osatekijöihin, eroaa samanlaisesta päätöksestä. Esimerkiksi lääkäri voi antaa erilaisen hoidon samaa sairautta poteville potilaille, vaikka tässä tilanteessa niin ei pitäisi käydä, vaan samaa sairautta potevat tulisi hoitaa samalla, tehokkaimmalla hoitomuodolla. Kahneman ym. (2009) toteavatkin, että ”epäjohdonmukaisuus on merkittävin heikkous epävirallisissa päätöksissä: saman taustatiedon esittäminen erilaisissa tilanteissa saa ihmiset useimmiten tekemään erilaisia päätöksiä.”

Intuitio tämän tutkimuksen takana

Kuten Kahneman ym. (2009) ovat todenneet sekä heuristiseen ja puolueelliseen (HP) että naturalistiseen päätöksentekoon (NPT) liittyen, että päätöksenteko kehittyy ajan myötä, ja että tehty päätös useimmiten eroaa eri tilanteessa tehdystä samasta päätöksestä – ei tämä tutkimus tee tähän teoriaan poikkeusta. NPT:n näkökulmasta tutkija kokee, että riittävän tieteellisen materiaalin läpikäytyä voidaan muodostaa tässä tutkimuksessa käytetty viitekehys, johon voidaan ottaa pääjaottelun mukaiset neljä komponenttia. Tämä siis tarkoittaa, että kun tutkija käy läpi tieteellistä materiaalia, hänen intuitio kehittyy ja hän oppii samalla hyvistä akateemisen maailman käytännöistä. Tämä on ensimmäinen syy, miksi tehty jaottelu on perusteltu.

Kahneman’n ym. (2009) vasta-argumentti NPT:lle on heuristisen ja puolueellisen päätöksenteon olemassaolo, jonka mukaan tässä tutkimuksessa tutkija ei välttämättä olisi tehnyt samaa pääjaottelua, jos tämä tutkimus oltaisiin toteutettu eri tilanteessa. Tämä on tietenkin totta, sillä on täysin mahdollista, ettei tutkimusta olisi toteutettu samalla pääjaottelulla. HP nojaa kuitenkin sellaiseen teoriaan, että päätöksentekijän intuitio olisi jollain tavalla merkittävästi vääristynyt, minkä takia ”väärä” päätös on tehty. Lisäksi nämä tutkitut tapaukset ovat pohjautuneet hyvin välittömiin tapahtumiin, jolloin harkinta-aikaa on ollut melko vähän. Tämän tutkimuksen teossa on käytetty runsaasti harkintaa ja ulkoista asiantuntijaa viitekehyksen hahmottamisessa, jolloin harkinta-aikaa on ollut varsin riittävästi ja tällä tavalla on ainakin pienennetty intuition mahdollista vääristymää ottamalla ulkoisen asiantuntijan mielipide huomioon.

Tutkimuksessa on näistä edellä mainituista syistä hyvä syy käyttää intuitiota pääjaottelun hahmottamisessa, sillä harkinta-aikaa on ollut riittävästi (NTP-näkökulma: päätöksenteko kehittyy ajan myötä) ja työhön on pyydetty apua ulkopuoliselta ja täysin riippumattomalta taholta (HP-näkökulma: päätöksentekoon liittyvä vääristymä on pienentynyt).

4 Tutkimustulosten raportointi

Tutkimustuloksia on käsitelty alla olevan taulukon mukaisesti, järjestyksessä vasemmalta oikealle. Siinä on jaoteltu kunkin osa-alueen tärkeimmät pääkohdat ja pyritty niputtamaan samaan kategoriaan toisiaan läheltä liippaavat aiheet. Taulukon tarkoituksena on helpottaa lukijaa ymmärtämään tutkimustulosten kokonaisuutta.

1. Kriittinen infrastruktuuri	Luokittelu organisaatiossa	Yhteishankkeet organisaatioiden välillä	Kriittisen infrastruktuurin regulaatio	
2. Organisaatio	Päätöksenteko & rakenteisiin liittyvät riskit	Järjestelmähankkeet & laadun varmistaminen & ulkoistukset	Menettelytavat & henkilöstön koulutus	Ulkoiset uhat & raportointi ylimmälle johdolle
3. Teknologia	Monitasoisten salasanojen käyttö & julkinen avain	Tietojen luokittelu	Tietoturvajärjestelmät & palvelinten turvallisuus	Ulkoisten uhkien kartoitus & tietoturvatarkastus
4. Ylin johto	Kriittisen tiedon tunnistaminen & luokittelu	Tietoturva: tietojen luottamuksellisuus, eheys & saatavuus	Toimintojen jatkuvuus & toipumissuunnittelu	Nykyisten kontrollien arviointi & uusien asettaminen

Taulukko 2: Empirian teemat jaoteltuna.

4.1 Kriittinen infrastruktuuri

Kriittiseksi infrastruktuuriksi luetaan yhtiöiden näkökulmasta viestintävälineet ja päätelaitteet, puhelin- ja tietoliikenneverkot sekä liiketoiminnassa käytetyt ohjelmat. Maksuliikenne ja pankkien tarjoamat palvelut kuuluvat myös kriittiseen infrastruktuuriin. Yhteiskunnan perspektiivistä kriittiseksi infrastruktuuriksi voidaan lukea sähköverkot, sähköjakelu, ja kaikki mikä liittyy niiden suojeluun. Lisäksi kriittinen infrastruktuuri käsittää rautatien, metron, satamat, ja kaikki sellaiset yhteiskunnan pyörittämiseen liittyvät asiat, joita ilman yhteiskunta ei toimisi.

Luokittelu organisaatioissa

Kriittiseksi infrastruktuuriksi luetaan yhtiöiden näkökulmasta tuotantolaitokset, koneet ja laitteet, tietoliikenneyhteydet (puhelin- ja internetyhteys), back-end-sovellukset (sisäiset ja ulkoiset palvelimet, esimerkiksi pilvi) ja kommunikointivälineet. Kaikki sellaiset asiat, joita tarvitaan yrityksen toiminnan pyörittämiseen. Eri yhtiöiden näkökulmasta kriittinen infrastruktuuri voidaan nähdä eri tavoin, esimerkiksi serveritilaa tarjoavia yhtiöitä voidaan pitää yksittäisen yhtiön näkökulmasta kriittisenä. Näistä asioista voidaan raportoida tilinpäätöstiedoissa, ja valistuneemmat organisaatiot tekevät kriittisyysluokitusta omaisuutensa suhteen.

”Kriittisen infrastruktuuriin liittyvä luokittelu juontaa juurensa ylimmän johdon jatkuvuussuunnitelmasta.”

Kriittisen infrastruktuurin luokittelu lähtee perinteisesti jatkuvuus- ja varautumissuunnitelman näkökulmasta ja kriittisiksi luetaan ne liiketoiminnot, jotka voisivat vaarantaa organisaation olemassaolon ja jatkuvuuden. Haastateltava kertoi yhdessä haastattelussa, että esimerkiksi ”eläkeyhtiössä tämä voisi olla eläkkeiden maksaminen, ja kaikki tähän liittyvät sovellukset ja järjestelmät.” Jos asiakkaat eivät saisi eläkkeitään tileilleen ilmoitettuna päivänä, tällä voisi olla eläkeyhtiön kannalta merkittävät seuraukset.

Yhteishankkeet organisaatioiden välillä

Kriittisen infrastruktuurin yhteishankkeita organisaatioiden välillä tarkoitetaan sellaisia yhteiskunnan projekteja, joilla tuotetaan esimerkiksi parempia tai turvallisempia viestintäyhteyksiä. Haastatteluista kävi ilme, ettei tämänkaltaisia yhteishankkeita juurikaan enää nykypäivänä ole. Yksi haastateltavista sanoi: ”Onhan meillä aikoinaan ollut World Wide Web-yhteishanke, silloin kun vielä viestintäyhteyksiä rakennettiin. Puhelinverkkojen rakentaminen on myös ollut tällainen, nykyään nämäkin on tosin yksityistetty.” Haastatteluiden pohjalta voisikin sanoa, että kriittisen infrastruktuurin yhteishankkeita on sen takia vähän Suomessa tai ne keskittyvät harvojen tekijöiden käsiin, sillä kriittiset infrastruktuurit ovat jo rakennettu aiemmin. Massiivista tuottavuuden hyppyä ei saada enää kriittisiä infrastruktuureita kehittämällä, vaan yhteiskunnan kannalta on parempi keskittyä muihin hankkeisiin.

Nykypäivän yhteishankkeet tietoliikenneyhteyksien rakentamisen suhteen voivat silti muokata yhteiskuntaa ja organisaatioiden toimintaa merkittävästi. Yksi haastateltava sanoi: ”Multitenant-palveluiden rakentaminen, esimerkiksi Googlen tai Amazonin tapauksessa, tarjoaa muille organisaatiolle hyötyjä oman ydinliiketoiminnan kehittämisessä. Tällöin tietoliikenneratkaisut hankitaan palveluna esimerkiksi IT-jäteiltä, jotka sitten huolehtivat koko tietoliikenneinfrastruktuurista.” Sama haastateltava jatkoi, että näitä hankkeita yleensä tehdään kustannussäästösyistä: isommalla skaalalla yhteisten konesalien ja internetyhteyksien hallinnointi tulee halvemmaksi.

Yhden haastateltavan mielestä yhteishankkeet ovat nykypäivänä yhä enemmän funktiokohtaisia ja näihin asioihin haetaan tietoa erilaisista seminaareista ja yhteistyötapahtumista. Esimerkiksi eri yritysten riskienhallinnasta vastaavat johtajat voivat kokoontua yhteen ja keskustella hyvistä käytännöistä esimerkiksi tietoturvauhkien vähentämisessä.

Regulaatio tietoliikenneratkaisujen kehittämisessä

Haastateltavat eivät jakaneet yhteistä näkemystä regulaation mahdollisista esteistä tai rajoitteista tietoliikenneratkaisujen kehittämisessä, vaan sen sijaan kysymystä lähestyttiin oman bisneksen näkökulmasta. Teollisuusalan haastateltava esimerkiksi totesi, että regulaatio asettaa ainakin kolmenlaisia vaateita omassa liiketoiminnassaan:

1. Yrityksen tuotantoon liittyvät vaateet: yrityksen tulee voida käsitellä oman BIM:n (building infstructure management software) avulla digitaalisessa muodossa sisään tulevia tarjouksia. Asiakkaiden tekemiin vaateisiin tulee pystyä vastata. **2.Henkilötietosuoja eli GDPR-asetus:** oman organisaation ja yhteistyökumppaneiden henkilökohtaiset tiedot tulee turvata ja niitä pitää pystyä käsitellä oikealla tavalla. **3.Taloudelliseen informaatioon liittyvät velvoitteet:** Patentti- ja rekisterihallitukselle tulee ilmoittaa tasaisin väliajoin taloustietoja. Lisäksi Verottajalle ja mahdollisille yhteiskumppaneille on tiedonantovelvollisuus sovituissa asioissa. Tietoliikenneratkaisuissa tulee varmentua tiedon oikeellisuudesta taloudelliseen informaatioon liittyen.

”Regulaatio tuo ainakin paljon velvoitteita yrityksille. Kriittisen infrastruktuurin aloista ainakin finanssi- ja teleala ovat hyvin säänneltyjä aloja. Itsessään regulaatio ei välttämättä aseta rajoitteita, vaan se pikemminkin hidastaa yritysten toimintaa. Kääntöpuolena on myöskin se, että regulaation tarkoituksena on suojata yrityksiä.”

4.2 Organisaatio

IT-asioita koskeva päätöksenteko

Vastuunjako IT-asioita koskevissa päätöksissä on perinteisesti jaettu IT-johtajan tai näitä asioita pohtivan osaston kesken, joka on saanut tehdä päätöksiä varsin itsenäisesti, kuten yksi haastateltavista ilmaisee. Nykyään ”bisnes-kriittiset IT-järjestelmät ovat bisneksen vastuulla ja IT-osasto sitten vastaa parhaasta toteutuksesta bisneksen näkökulmasta. Järjestelmäkehitys tehdään yhä useammin liiketoiminnan ehdoin, jolloin aloitteet tulevat sieltä. Tästä seuraa tehokkuutta, sillä jokainen organisaation liiketoimintayksikkö voi keskittyä omaan tehtävään, mutta samalla vuoropuhelu IT:n ja bisneksen välillä korostuu.”

Saman suuntaisia vastauksia tuli myös muilta haastatelluilta. Yksi haastatelluista nosti tärkeäksi aiheeksi IT-hankintojen strategisuuden: ”Riippuen IT-hankinnan strategisuudesta, pitoajasta ja hankinnan suuruudesta, että käykö hanke läpi perinteisen investointihankkeen prosessin. Pienemmissä hankkeissa IT-johto voi tehdä omat päätökset. - - Mitä enemmän hankinta koskee yhtiön omaa liiketoimintaa, niin sitä enemmän liiketoimintayksikön johtaja on vastuussa IT-hankintoja koskevista päätöksistä. - - Tärkeään rooliin tällöin nousee IT- ja liiketoimintayksikön vuoropuhelu.”

Toimiala ja yrityksen koko vaikuttavat myös varsin suuresti siihen, millä tavalla IT-asioista päätetään. Lisäksi yksi haastateltava avasi oman organisaation päätöksentekoa: yhtiössä on valmisteleva IT-kaksikko, jonka vastuulla on neuvotella yhteistyösopimuksia toimittajien kanssa, määritellä laadulliset asiat sopimuksiin liittyen ja esitellä nämä talousjohtajalle, joka tekee lopulliset päätökset. ”Hallitus ja toimitusjohtaja vastaa viime kädessä siitä, että yhtiö täyttää lait ja asetukset, ja että yhtiön omaisuus on turvattu. - - Meillä on talousjohtajan alle organisoitu kahden hengen IT-tiimi, joka valmistelee yhtiötä muuttuvaan maailmaan ja miettii mahdollisia uusia toimittajia, jotka voisivat hoitaa tietyt asiat paremmin kuin nykyiset kumppanit.”

IT-hankintojen prosessikuvaus päätöksenteon näkökulmasta

Operatiivinen yksikkö	IT-osasto (esim. kahden hengen IT-tiimi)	Paras mahdollinen IT-hankinta
1. Tekee aloitteen. 3. Kertoo omista tarpeistaan IT-osastolle.	2. Osallistuu aloitteen tekemiseen yhdessä operatiivisen yksikön kanssa. 4. Määrittelee IT-vaatimukset. 6. Valvoo tietoturvaa hankkeen aikana.	5. IT-osasto tekee ehdotuksen parhaasta mahdollisesta hankinnasta.
Hankintayksikkö / Ohjausryhmä		
- Osallistuu kilpailutukseen, sopimusneuvotteluihin ja valvoo hankkeen etenemistä. - Puhtaasti neuvotteleva osapuoli, joka vastaa taloudellisista asioista.		
Mitä tulee ottaa huomioon ennen kun sitoudutaan sopimukseen:		
- Tehdään pilottikokeiluita mahdollisten palveluntarjoajien kanssa parhaan ratkaisun löytämiseksi. - Hyvin tarkka määrittely vastuista: mistä kaikesta palveluntarjoaja vastaa esimerkiksi tietovuodon tapauksessa. - IT-tiimi määrittelee hyväksyttävät riskit tietoturvan suhteen, jotka ylin johto hyväksyy.		

Taulukko 3: Prosessikuvaus IT-hankintojen tietoturvasta tehtyjen haastatteluiden pohjalta.

IT-osaston ja tietoturvasta vastaavan tiimin eriyttäminen

Aiemmin tietoturva-asioista ja muusta IT:stä tehtävät päätökset valmisteltiin samassa funktiossa, mutta nykyään tietoturvan katsotaan liittyvän kaikkiin liiketoimiin eikä ole sellaista bisnesaluetta, johon tietoturva ei jollain tavalla liittyisi. Tästä syystä osa yrityksistä on sitä mieltä, että tietoturvan tulisi olla osa kaikkea tekemistä ja tietoturvapäätökset tulisi tehdä jokaisen liiketoimintayksikön näkökulmasta sopimaan juuri siihen tiettyyn tehtävään. IT-osaston tehtäväksi tulee yhä enemmän eri teknologioiden hallinnointi ja yhteensovittaminen.

”Tietoturvaosaaminen olisi hyvä keskittää, mutta samalla tietoturva tulisi hajauttaa koskemaan jokaista liiketoimintayksikköä.”

Liiketoimintayksiköiden välillä tapahtuva tiedon välitys – kriittinen ja haavoittuva kohta?

Matriisiorganisaatioissa tieto saattaa ylittää liiketoimintayksiköiden rajat, jolloin näiden rajapinnoissa tapahtuva tiedon vaihto voi olla kriittinen ja haavoittuva kohta. Lisäksi rajapinnassa toimivan henkilöstön valtuudet ja oikeudet saattavat aiheuttaa vaarallisia työyhdistelmiä, jos näihin asioihin ei ole otettu kantaa organisaatiorakenteeseen liittyvissä päätöksissä. Yksi haastateltava nosti mahdollisuuden hahmottaa liiketoimintayksiköiden välisiä ongelmakohtia ristiintaulukoimalla erilaisia työtehtäviä ja vastuita (RACI-malli). RACI-mallia voidaan käyttää apuna myös investointeja koskevassa päätöksenteossa.

RACI-malli: ”Ihmisten tehtävien jakaminen on hoidettu niin, että osa ihmisistä toteuttaa, osaa informoidaan (, ja joilla ei ole sanavaltaa), ja osaa ihmisistä tulee konsultoida päätöksessä ja kysyä mielipidettä, mutta joku toinen tekee lopullisen päätöksen. - - Kun kyse on isoista investoinneista (+10 miljoonan hankinnoista) ja taloudellinen pitoaika on useita vuosia, RACI-malli on periaatteessa ainoa mahdollinen tapa onnistua investoinnin toteuttamisessa läpinäkyvästi ja luotettavasti.”

	Työntekijä 1	**Työntekijä 2**	**Työntekijä 3**	**Työntekijä 4**	**Työntekijä 5**
Työtehtävä 1	I	I	C	A	R
Työtehtävä 2	I	A/R	-	-	I
Työtehtävä 3	A/R	C	I	-	R
Työtehtävä 4	C	A	R	R	C

Taulukon mukaan työntekijä 1 toimii työtehtävissä 1 ja 2 tiedotettavana henkilönä, työtehtävässä 3 vastuussa olevana (accountable) sekä vastuullisena (responsible) henkilönä. Lisäksi hän toimii neuvojan roolissa työtehtävässä 4. R = responsible (vastuullinen), A = accountable (vastuussa oleva, tilivelvollinen), C = consulted (neuvoja), I = Informed (tiedotettava).

Taulukko 4: Esimerkki RACI-mallista.

Yksi haastateltavista nosti esiin käyttövaltuushallinnan vaarallisten työyhdistelmien ehkäisyssä, mikä tarkoittaa, että jokaista työtehtävää kohden tulisi selvittää mahdolliset uhat organisaation näkökulmasta. Hän tosin myös totesi, että on erityisen haastavaa rakentaa hyvin hallittavaa tietoturvallista organisaatiota, jossa on paljon limittäisiä ja lomittaisia liiketoimintoja. Haastateltavat toivat moneen

kertaan eri vaiheissa esille, että organisaation ongelmakohtia voidaan jälkikäteen tutkia sisäisen tarkastuksen keinoin esimerkiksi lokitietoja tutkimalla. Näin organisaatio voi asettaa uhan työntekijöitä kohtaan jäädä kiinni, jonka voidaan nähdä vähentävän vaarallisten työyhdistelmien kautta tulevaa uhkaa.

Tietoturvan varmistaminen järjestelmähankkeissa

Tietoturvan vaatimustaso järjestelmähankkeissa riippuu hyvin suuresti siitä, minkälaista järjestelmää ollaan hankkimassa. Esimerkiksi yksi haastateltavista kertoi: ”Hankittava laskentajärjestelmä ei todennäköisesti ’puhu’ ulkomaailman kanssa, ja tästä syystä laskentajärjestelmä ei ole samalla tavalla ulkoisten hyökkäysten kohteena. - - Järjestelmää tulisi suojata niistä lähtökohdista, miten järjestelmä näkyy ulospäin.” Lisäksi täytyy huomioida tietojen sensitiivisyys: talousdata esimerkiksi tarjouspyyntöjen osalta ei ole yhtä sensitiivistä tietoa kuin käyttäjien henkilökohtaiset tiedot.

Hankkiva organisaatio voi tehdä vaatimusmäärittelyä palveluntarjoajalle jo tarjouspyyntövaiheessa. Tällöin pienennetään riskien realisoitumisen todennäköisyyttä, kun etukäteen on jo huomioitu tiettyjä järjestelmiin liittyviä riskejä. Lisäksi organisaatio voi tehdä auditointeja meneillään olevaan hankkeeseen ja määritellä vaatimustasoja uudelleen. Vaihtoehtoisesti organisaatio voi ulkoistaa auditointien tekemisen ulkopuoliselle yritykselle ja pyytää ulkopuolista neuvonantajaa antamaan puolueettoman näkemyksen vaatimustasojen määrittelystä.

”Tarjouspyynnöissä voidaan viitata esimerkiksi ISO 27001-standardiin tai Katakri-viranomaisauditointiin laadun varmistamiseksi.”

Organisaation toimialasta ja kokoluokasta riippuen auditointien ja tietoturvan varmistaminen voidaan ulkoistaa kokonaisuudessaan ulkoisen palveluntarjoajan vastuulle. Haastatteluissa kävi ilmi, että yhden organisaation mukaan palveluntarjoaja on vastuussa esimerkiksi päätelaitteiden tietoturvasta, ja että ulkopuolinen konsultti käy arvioimassa hankkeiden tietoturvaa ja arkkitehtuuria tasaisin väliajoin yhtiön toimiala ja kokoluokka huomioiden.

Lisätöiden hyväksyminen IT-hankkeisiin

Liiketoimintayksikön johto saattaa huomata IT-hankintaprosessin aikana, että hankittava järjestelmä tai sovellus ei sovellu sellaisenaan organisaation käyttöön, vaan siltä voidaan vaatia joitakin lisäkyvykkyyksiä. Yksi haastateltava sanoi, että jotta organisaatio voisi varautua mahdollisiin lisätöihin, on näistä kustannuksista tärkeää ottaa jo etukäteen selvää. Lisäksi perinpohjaisella valmistelulla ja käyttäjien sitouttamisella prosessiin yleensä saadaan parempia tuloksia aikaan. Kommunikaation tärkeys eri toimijoiden välillä nousee merkittävään rooliin.

Perinteisesti IT-hankkeiden budjetit ja investointikohteet päätetään kerran vuodessa, kuten kaksi haastateltavaa sanoi. Selville budjetin ylityksille haetaan lupaa hallitukselta, mutta pienimmille ylityksille johtoryhmä voi antaa luvan.

Yksi haastateltava nosti hankintayksikön/ohjausryhmän tärkeyden lisätöiden ja koko hankinnan seurannassa. Organisaatiossa on yleensä määritelty ohjausryhmä, jonka tehtävänä on seurata projektin edistymistä, pitää kirjaa jo tehdyistä töistä, ja töistä jotka on tilattu mutta ei vielä toimitettu. Ohjausryhmä selvittää lisätöiden tarvetta koko hankkeen aikana, ja valitun toimittajan tulee ilmoittaa niistä asioista, jotka eivät sisälly sopimukseen ja jotka tulee käsitellä erillisinä lisätöinä. Lisätyöilmoitusten jälkeen nämä käsitellään ohjausryhmässä ja tämän jälkeen tilataan organisaation vaatimusten mukaan. Ohjausryhmän tehtävä on tehdyn tilauksen jälkeen seurata ja valvoa hankkeen toteutumista.

Tietoturvan huomiointi ulkoistuksissa

Eräs haastateltavista sanoi, että yritysmaailmassa mennään yhä enemmän ulkoistuksien suuntaan, jolloin organisaatiot pyrkivät tehostamaan niiden operatiivista toimintaa ja tukitoiminnot hankitaan toisilta yrityksiltä. ”Perinteisesti ulkoistuksiin liittyvää uhkaa on yritetty rajata sopimuksin, esimerkiksi niin että sopimuksissa on vaadittu tietoturvan taso. Nykyisin ulkoistavat organisaatiot ottavat selvää siitä, miten palveluntarjoaja ottaa tietoturva-asiat huomioon tarjoamissaan järjestelmissä ja sovelluksissa.” Enää ei siis tehdä pelkästään sopimuksia ulkoistajien kanssa ja toivota että mitään ei tapahtuisi, vaan organisaatiot ottavat proaktiivisemman asenteen selvittää palveluntarjoajan prosesseja ja näiden tietoturvan tasoa. Haastateltava sanoo, että näin yritykset voivat minimoida ulkoistuksiin liittyviä riskejä.

Toinen haastateltava nosti ulkoistuksen kohteen vaikuttavan tietoturvavaateisiin. Esimerkiksi kirjanpidon ulkoistaminen vaatii erilaisen tietoturvatason kuin esimerkiksi henkilötietojen käsittelyn ul-

koistaminen. ”Hankintavaiheessa tulee selvittää, minkälaisten putkien läpi data kulkee, missä datakeskukset sijaitsevat, miten data-sensitiivisyys tulisi ottaa huomioon, ja kuka datakeskuksia valvoo ja minkälaisin valtuuksin (hän ei esimerkiksi voi nähdä todellista dataa [objekteja], vaan esimerkiksi kryptattua dataa).” Ulkoistuksiin liittyvät tietoturvavaatimukset tulee määritellä jo hankintavaiheessa ja meneillään olevaan hankkeeseen voidaan tehdä auditointeja ja määritellä vaatimustasoja uudelleen. Vaihtoehtoisesti voidaan pyytää jokin ulkopuolinen yritys tekemään vaadittavat auditoinnit ja varmistamaan tietoturvan taso.

Toimintatapojen yhtenäisyyden varmistaminen

Toimintatapojen yhtenäistämisellä pyritään varmistumaan, että samaa työtehtävää tekevät ihmiset tekevät työtä samalla standardoidulla tavalla. Muussa tapauksessa tietoja voisi hävitä tai tietojen vaihto eri työvaiheiden välillä voisi olla puutteellista, jolloin organisaation toiminta voisi vaarantua. Haastateltavat olivat varsin yksimielisiä, että ylimmän johdon vastuulla on ohjeistuksien ja hyvien tapojen ja käytäntöjen synnyttäminen organisaatioon.

”Ensin sovitaan, miten tietyissä työtehtävissä toimitaan, ja sitten luodaan työvälineet. Työvälineiden käyttöä ohjeistetaan dokumentaation avulla ja tietyin väliajoin testataan, miten työntekijät niitä käyttävät. Lokit varmistavat, että sovittujen periaatteiden mukaan on toimittu.”

”Hallinnointimallin avulla tästä pidetään huolta. Testaukset ja kehitysympäristöt tulee olla rakennettu niin, että tietoturvaratkaisut toimivat. Kyse on loppupeleissä arkkitehtuuriratkaisusta, ja siitä että kaikki arkkitehtuurista vastaavat toimivat sovittujen toimintatapojen mukaan.”

”Haasteita ilmenee aina silloin, kun prosesseja ei ole kuvattu. Yleinen tapa toimia on laittaa prosessien dokumentaatio, politiikat ja ohjeet yrityksen intraan. Aina tämä ei ole varmin tapa varmistaa toimintatapojen yhtenäisyys.”

Kriittisten työtehtävien valvonta/seuranta tietojärjestelmän avulla

”Mitä pienempi organisaatio on kyseessä, sitä vähemmän käyttöoikeuksilla pystyy rajata kriittisiä työtehtäviä, sillä työntekijät saattavat tehdä päällekkäisiä työtehtäviä tai heillä voi olla samat oikeudet työtehtävien tekemiseen”, kertoi yksi haastateltavista, kun hän viittasi kriittisten työtehtävien valvontaan. Yksi tapa varmentua työtehtävien oikeasta suorittamisesta on esimerkiksi lokien seuraaminen ja jälkikäteiskuittauksien hallinta. Tällöin ihmisillä on tiedossa mahdollinen kiinnijäämisen riski, mikä voi olla riittävä toimenpide estää väärinkäytöksiä tapahtumasta. Toinen tapa seurata samaa asiaa on esimerkiksi selvittää, kuinka paljon asioita on tehty sovitulla järjestelmällä. Tällainen voisi olla tarjouspyyntöjen tekeminen tietyllä järjestelmällä, joka kirjaa ja seuraa kaikkea toimintaa tähän tiettyyn tarjoukseen liittyen. Loppujen lopuksi kriittisiä työtehtäviä ”pystytään varsin pitkälle hoitamaan järjestelmien avulla”, eräs toinen haastateltavista kertoo.

Järjestelmiin voidaan myös rakentaa sellaisia toimintoja, jotka osaavat hälyttää mahdollisen uhan ilmaantuessa. Riittävän suuri rahatransaktio voi olla tällainen, ja nämä hälytykset voidaan asettaa koskemaan esimerkiksi yksittäisiä suuri laskuja tai suurta määrää samaa toimittajaa koskevia pieniä laskuja. Lisäksi yksi haastateltavista nosti toimittajien hallinnan keskeiseksi teemaksi väärinkäytöksien ehkäisemisessä: ”Perinteisesti, kun puhutaan toimittajien hallinasta, niin toimittajan saa perustaa yksi henkilö ja pankin tiedot perustaa toinen henkilö. Lisäksi järjestelmä pitää rakentaa niin että toimittajan perustanut henkilö ei pääse muuttamaan pankkitietoja.”

”Periaatteessa nämä voidaan jakaa estäviin toimiin ja jälkikäteistarkastukseen.”

Varahenkilöjärjestelyt

Varahenkilöjärjestelyillä tarkoitetaan sellaisia järjestelyitä, joilla turvataan organisaation jatkuvuus esimerkiksi henkilöstön vaihtuessa, henkilöstön ollessa sairaana tai muuten kyvytön olemaan organisaation palveluksessa sovittuna työaikana. Haastateltavat jakoivat vahvan konsensuksen varahenkilöjärjestelyiden tärkeydestä, mutta he olivat eri mieltä varahenkilöjärjestelyiden toteuttamisesta.

Haastatellut olivat sitä mieltä, että organisaation koko ja toimiala vaikuttavat varahenkilöiden määrittelyyn. Pienemmissä organisaatioissa ei välttämättä ole määrittelyä lainkaan, sillä se voisi tuoda byrokraattisen ja hidastavan tason liiketoimintaantoimintaan. Tällaisissa pienissä organisaatiossa voikin olla niin, että kaikki työntekijät hoitavat kaikkia työtehtäviä. Haastateltavat myös sanoivat, että pienemmät organisaatiot ”yleensä ulkoistavat nämä toiminnot organisaatioille, joilla on esimerkiksi

24-tunnin monitorointi.” Haastatellun mielestä paras ja tehokkain tapa toimia, on antaa bisnesvastuu organisaatiolle ja antaa muiden hoitaa varahenkilöjärjestelyt.

”Yhtiössä on henkilöstön suhteen hyvin pieni vaihtuvuus ja työsuhteet ovat pitkiä, mikä osaltaan on vaikuttanut siihen, ettemme ole joutuneet testaamaan varahenkilöjärjestelyiden toimivuutta.” Tämä voi olla ongelma tietoturvan näkökulmasta, sillä prosesseja ei ole välttämättä testattu riittävästi uhkatilanteiden suhteen. Lisäksi hyvin pitkillä työsuhteilla voi olla bisnesvaistoa hämärryttävä vaikutus, mikä voi johtaa organisaation jatkuvuus ongelmiin pitkällä aikavälillä.

Milloin eri tahojen identiteetin varmentaminen on tärkeää, ja miten se kannattaa tehdä?

Identiteetin varmentaminen on silloin tärkeää, kun tapahtuu jokin vastuisiin, velvollisuuksiin ja oikeuksiin liittyvä vaihtokauppa. Esimerkiksi palkan maksu tai sopimuksen allekirjoittaminen voisi olla tällainen, sillä kumpaankin tapaukseen liittyy velvoitteen täyttäminen sekä oikeus resurssin käyttöön. Lisäksi haastateltavat nostivat asiakastietojen käsittelyyn liittyvät haasteet: silloin on käytettävä vahvaa tunnistusta, kun jaetaan asiakasta koskevaa tietoa esimerkiksi puhelun välityksellä.

Eräs haastatelluista nosti tärkeäksi tapahtumaksi asiakassuhteen luomisen yhteydessä tehdyn identiteetin varmentamisen. Heidän organisaatiossa käytetään eri prosessien eri vaiheissa neljän-silmänperiaatetta, mikä tarkoittaa esimerkiksi asiakassuhteen luomisen yhteydessä sitä, että sama ihminen ei voi perustaa asiakasta ja hyväksyä sitä, vaan hyväksymisen hoitaa toinen ihminen. Tällöin kukaan ei voi perustaa uutta asiakasta, ja laittaa pankkitiliksi omaa tiliään, koska toinen ihminen lopulta tekee lopullisen hyväksynnän.

”Asiakastietojen muuttaminen vaatii myös useamman ihmisen toimia.”

Koulutus ja tietoisuuden lisääminen: tietoturvaharjoituksien ja -koulutuksien järjestäminen

Tietoturvaharjoitus on konkreettinen tapa lähestyä mahdollista uhkaa turvallisissa olosuhteissa. Tietoturvaharjoitus alkaa yleensä ulkopuolisen organisaation tekemällä kuvauksella alkuvaiheen tilanteesta ennen kriittistä tilannetta. Tätä vaihetta seuraa toimintavaihe, jossa ulkopuolinen voi ohjeistaa organisaation työntekijöitä toimimaan oikealla tavalla kriisitilanteessa, tai vain seurata sivusta organisaation toimintaa. Kuvitteellisen tilanteen rauettua ulkopuolinen organisaation antaa palautetta työntekijöille heidän toimistaan ja antaa parannusehdotuksia.

Haastateltavat kommentoivat, ettei tietoturvaharjoituksia juurikaan pidetä. Eräs haastateltavista kommentoi: ”Niitä ei tehdä niin paljon kun ehkä pitäisi. Ylimmän johdon harjoituksia on järjestetty, ja näissä on heitetty johdolle jokin case, jonka jälkeen on katsottu, miten ylin johto on tästä selviytynyt. Ylimmälle johdolle näitä harjoituksia järjestetään enemmän, mutta siitä alaspäin harjoitusten järjestäminen on harvemmassa.” Sama haastateltava kommentoi, että tietoturvauhkia käsitteleviä harjoituksia ei ainakaan vielä tehdä samalla frekvenssillä kuin esimerkiksi paloturvallisuusharjoituksia.

”Koulutuksia järjestetään, kun organisaatio ottaa uusia työkaluja otetaan käyttöön: näitä testataan esimerkiksi e-learning-alustojen ja osaamistestien avulla. Painotus muuttuu tietoturvaharjoitusten suuntaan tulevaisuudessa.”

”Tärkeä aihe on disaster recovery, joka tarkoittaa, että organisaation tulee testata oma datan käsittely, jos sattuu virhe/hyökkäys/ongelma X. Lisäksi organisaation tulisi selvittää, miten kaatuneista järjestelmistä data saadaan takaisin ilman, että siitä puuttuu joitakin tietoja.”

Kilpailuympäristön asettamat paineet: organisaation aineettomasta omaisuudesta hyötyvät tahot

Haastateltavat olivat varsin yksimielisiä siitä, että tuotekehitykseen ja siihen liittyvä osaaminen on voisi väärissä käsissä aiheuttaa kohtalokkaita seurauksia organisaation jatkuvuuden kannalta. ”Jos jokin toinen yhtiö saisi tuotekehitystä koskevia dokumentteja omiin käsiin, tämä yhtiö voisi saada huomattavan etulyöntiaseman verrattuna tuotekehitystä tekevään yhtiöön, sillä se ei ole joutunut käyttämään juurikaan resursseja omaan kehitystyöhön. Yleensä tuotekehitys on yhtiön näkökulmasta kaikista eniten resursseja vievää toimintaa.” Lisäksi tuotekehitykseen liittyvä aineettoman omaisuuden syntyminen on organisaation näkökulmasta yksi pidemmän aikavälin kilpailukyvyn takaaja, siksi tämän osaamisen vuotaminen ulkopuolisille sidosryhmille heikentää organisaation jatkuvuutta.

”Tuotekehityksen liittyvistä dokumenteista voi olla hyötyä ulkopuoliselle sidosryhmälle, mutta muuten datan vuotaminen ulkopuolelle on tapauskohtaista: riippuu millaista dataa vuotaa ja millaiselle sidosryhmälle.”

Megatrendien vaikutus IT-järjestelmiin organisaatioissa

Digitaalisuus ja digitalisaation eteneminen ovat selkeitä kehityssuuntia tietojärjestelmien kehittymisessä ja lisäksi datan eksponentiaalinen kasvu on synnyttänyt organisaatioissa kysynnän datan analysoinnille. Lisäksi haastateltavat nostivat ympäristövastuullisuuden ja ilmastonmuutokseen liittyvät seikat tärkeiksi asioiksi, joiden nähdään muokkaavan merkittävästi markkinoiden kilpailuasetelmaa tulevaisuudessa. Esimerkiksi organisaation tuottama hiilijalanjälki jonkin tuotteen suhteen voi muodostua kuluttajien kysyntää ohjaavaksi tekijäksi.

Yksi haastateltavista varoitti nykyisten uusien teknologioiden vaaroista, joista merkittävin on IoT, asioiden internet. ”IoT:hen sisältyy suuria tietoturvariskejä, jotka liittyvät IoT-teknologian langattomuuteen, keveisiin ja vähän sähköä kuluttaviin laitteisiin. Johtuen edellä mainituista asioista, myös tietoturvaratkaisut on rakennettu keveäksi ja vähän sähköä käyttäväksi.” Lisäksi IoT-laitteisiin kohdistuu kovat hintapaineet, sillä mitä halvempi laite tuotetaan, sitä todennäköisemmin laite voidaan ottaa käyttöön mitä monimuotoisemmissa paikoissa. Tällöin tietoturva-asiat voivat jäädä toissijaisiksi asioiksi.

”Asioiden internetin yleistymistä voidaan pitää suurena tietoturvariskinä tällä hetkellä.”

Toinen haastateltavista kertoi konkreettisen esimerkin, miten teknologia muuttaa teollisuuden alaa: ”Perinteisesti asentaja on saanut hyvin vapaat kädet päättävät, millaisia putkia ja pattereita asuntoon asennetaan. Nykyään taloja suunnitellaan kokonaisvaltaisemmin (**BIM-työkalulla**) ja nämä aiemmin asentajan tekemät päätökset tehdään jo suunnittelupöydällä suunnittelijan tai arkkitehdin toimesta.” Haastateltava myös pohti sitä, mikä on tukkuliikkeiden merkitys tulevaisuudessa, kun päätökset tehdään jo paljon ennen, kun taloa on alettu rakentaa. On hyvin mahdollista, että esimerkiksi putkia ja pattereita valmistava yritys myisikin suoraan rakennusliikkeelle, jolloin tukkuliikkeen merkitys koko tuotantoketjussa vähenee tai jopa poistuu kokonaan tämän organisaation tapauksessa.

Sama haastateltava mainitsi myös teollisuus- ja rakennusalaan liittyvän megatrendin, sillä nämä alat tuottavat merkittävän määrän hiilidioksidipäästöistä, ja voisi kuvitella, että näiden alojen hiilidioksidipäästöjen vähentäminen olisi EU-päättäjien prioriteettilistalla hyvin korkealla. Pitkässä juoksussa rakennus- ja teollisuusalan voidaan siten nähdä muuttuvan hiiliystävällisemmiksi aloiksi.

Tietoturvasta raportoiminen ylimmälle johdolle

Tietoturvasta raportoiminen nähtiin ennen kaikkea reaktiivisena toimintana, jolloin ylimmälle johdolle yleensä raportoidaan sellaisissa tilanteissa, kun on tapahtunut jotain poikkeavaa. Tulevaisuuden tapahtumien ennustaminen on usein hankalaa, mutta näitä tapahtumia varten voidaan luoda poikkeuskäytäntöjä, jotka pyöräytetään käyntiin ongelmatilanteen ilmetessä. Nämä poikkeuskäytännöt voivat pitää sisällään viestintää, raportointia ja muita asioita, joita pitää ottaa huomioon. Lisäksi tiedon pitää saavuttaa ylin johto mahdollisimman nopeasti, jotta voidaan reagoida esimerkiksi median suuntaan. Sosiaalisen median aikakaudella nopeus vain korostuu, jotta riskejä voidaan rajata ja väärinkäsityksiltä välttyä.

Eräs haastateltavista kertoi, että ongelmien ilmetessä ne nostetaan säännöllisten kokousten kautta pöydälle ja näistä kommunikoidaan henkilöstölle. Lisäksi heidän (ja monella muulla) organisaatiolla on tiettyjä varoittimia jotka varoittavat, jos esimerkiksi järjestelmään yritetään tulla jostain sellaisesta maasta, jossa yrityksellä ei ole omaa toimintaa. Tietojenkalastelu-viesteistä (**phishing**) tulee automaattisia varoituksia ja näistä puhutaan henkilöstön kanssa jatkuvasti.

”Raportointi on oikeastaan nähtyjen uhkien ja nykyisen tilanteen raportointia ylimmälle johdolle, sillä johto ei välttämättä ymmärrä teknisempiä asioita. Raportointi on reaktiivista, vaikka alun perin näitä asioita on mietitty proaktiivisesti.”

4.3 Teknologia

Monitasoisten salasanojen käyttö

Monitasoiset salasanat auttavat organisaatiota suojaamaan eri tasoista tietoa sekä vähentämään vaarallisten työyhdistelmien mahdollisuutta väärinkäytöksille. Lisäksi monitasoisten salasanojen käyttö auttaa huolehtimaan organisaation jatkuvuudesta: esimerkiksi, jos yksi monitasoisen salasanaketjun salasanoista vaarantuu, ei tietoihin välttämättä päästä käsiksi, vaan se vaatisi jonkin toisen salasanan vuotamisen samanaikaisesti. Monitasoisten salasanojen käyttökohde voisi olla esimerkiksi salaisiin tietoihin pääseminen, joihin vaaditaan vahvaa tunnistamista.

Haastateltavien mukaan monitasoisia salasanoja kannattaa käyttää sellaisissa tilanteissa, kun käyttäjä toimii organisaation ulkoverkossa tai jos tiettyyn järjestelmään liittyy hyvin laajat valtuudet toimintoihin tai organisaation dataan liittyen. Eräs haastateltavista kertoi, että tällaisia tilanteita varten voidaan käyttää vahvaa tunnistamista, joka voisi ilmentyä esimerkiksi puhelimeen lähetetyn viestin muodossa. Kaksivaiheisesta tunnistamisesta puhutaan silloin, kun järjestelmään pääsemiseksi vaaditaan käyttäjätunnus/salasana-yhdistelmä ja tämän lisäksi vielä vahva tunnistaminen.

Haastateltavat kertoivat, että pörssiyhtiöillä kaksivaiheista tunnistamista voidaan käyttää hallitusmateriaalien suojaamiseksi. Yrityskauppaneuvottelutilanteessa voidaan myös käyttää monitasoisia salasanoja salaisten tietojen suojaamiseksi. Periaatteessa kaikenlainen organisaation määrittelemä salainen sisäinen tieto kannattaisi suojata monitasoisilla salasanoilla.

”Ulkoverkosta tuleville yhteyksille on aina tehtävä vahva tunnistus ja VPN-yhteys.”

Julkisen avaimen infrastruktuuri

Julkisen avaimen infrastruktuuri on sellainen tietojärjestelmiin liittyvä rakennelma, johon liittyy julkisia ja yksityisiä avaimia. Näitä avaimia käytetään esimerkiksi salaamaan tiedostoja verkon yli toimiessa, kun halutaan lähettää tiedosto tietylle käyttäjälle. Tiedoston saaja voi purkaa salauksen omalla yksityisellä avaimella, jolloin kukaan muu ei teoreettisesti pysty purkaa tätä salausta.

Haastateltavat kertoivat, että tyypillisin tapa huolehtia tietojen luottamuksellisuudesta on estää pääsy tietoihin perinteisten salasanojen avulla. Kehittyneempiä teknologioita ei juurikaan käytetä, ja haastateltavat kertoivat, että joissakin tapauksissa tietoja ei suojata lainkaan. Periaatteessa tämä on täysin ymmärrettävää, jos organisaation käsittelemät tiedot eivät sisällä sensitiivistä dataa asiakkaita tai erilaisia projekteja kohtaan. Kukaan ei välttämättä tee mitään esimerkiksi yrityksen tarjouspyynnöllä.

Tietojen luokittelu organisaatioissa

Monitasoisten salasanojen yksi käyttökohde on organisaation salaisiin tietoihin pääseminen. Lisäksi käyttövaltuushallinnalla on tietojen luokittelussa merkittävä rooli, sillä käyttövaltuushallinnalla pyritään selvittämään, kenelle kaikille annetaan valtuudet lukea ja muokata tietoa. Eräs haastateltavista kertoi tietojen luokittelusta seuraavaa: ”Tämänkaltainen luokittelu on ihan yleisessä käytössä. Esimerkiksi salainen-sisäinen-julkinen.”

Toinen haastateltavista sanoi, että dokumentinhallinnassa salainen-julkinen-asteikko voisi toimia, mutta varsin harvassa organisaatiossa todella käytetään tämänkaltaista luokittelua. Sen sijaan tärkeämpää on miettiä, mihin kaikkiin toimintoihin todella tarvitaan vahvoja salasanoja. Tällöin organisaatio ei tee päätöksiä teknologiasta jonain päämääränä, vaan teknologiset päätökset sitoutuvat organisaation tekemiseen, nostavat tietoturvan tasoa ja luovat tehokkuutta.

Organisaatioiden käyttämät tietoturvanhallintajärjestelmät

Haastateltavien mielestä datan suojaaminen ja yhteyksien hallinnointi ovat tietoturvanhallintajärjestelmän kannalta tärkeimmät ominaisuudet. Tietoturvanhallintajärjestelmään voidaan lukea myös käyttäjien laitteita suojaavat virusturvaohjelmistot sekä palvelimien omat virusturvaohjelmistot. Yksi haastateltavista kertoo: ”Formaliteetin taso vaihtelee yhtiökohtaisesti. Joillakin on esimerkiksi ISO-standardiin perustuvia järjestelmiä. - - Joillakin taas on yksittäisiä poliitikkoja ja ohjeita.”

Toinen haastateltavista heidän ohjeistuksista: organisaation työntekijät eivät saa esimerkiksi käyttää Applen sähköpostisovellusta, sillä organisaation oma tietoturvatiimi on todennut sen tietoturvauhaksi. Lisäksi toinen haastatelluista kertoo, että tarvittavat tietoturvaohjelmistot voidaan ostaa tietoturvayhtiöiltä, ja näiden hallinnointi on ulkoistettu toisen yhtiön hoidettavaksi.

Palvelinten turvallisuus

Palvelinten turvallisuus liittyy organisaatioiden jatkuvuus- ja varautumissuunnitteluun, sillä palvelimet ovat kriittinen ja mahdollisesti haavoittuva kohta organisaatioiden toiminnassa. Perinteisesti organisaatiot ovat omistaneet itse käyttämänsä konesalit, joissa palvelimet sijaitsivat. Nykyään käytetään kuitenkin luotettavia palveluntarjoajia, jotka huolehtivat näiden palvelinten turvallisuudesta. Eräs haastateltavista sanoi, että yksittäisen organisaation näkökulmasta palvelimet tulisi pitää kahdennettuina ja erottaa toisistaan erillisille maantieteellisille alueille, jotta palvelimilla pyörivät sovellukset ja data välttäisivät esimerkiksi luonnonkatastrofien tai tulipalojen vaikutukset.

Eräs haastateltavista sanoi, että voi olla järkevämpää valita mahdollisimman iso palvelintoimittaja, sillä näillä tietoturvan taso, palomuurit ja tavat toimia ovat todennäköisesti paremmalla tasolla kuin pienemmän palvelintoimittajan vastaavat palvelut. Lisäpalveluna organisaatiot voivat pyytää palvelintoimittajaa salaamaan tiedostot sekä tietokannat palvelimilla, jolloin voidaan välttää mahdollinen tietovuoto kolmansille osapuolille.

Ulkoisten uhkien riskikartoitus

Ulkoisia riskejä pyritään tunnistamaan toimialasta riippuen ja lisäksi riskikartoituksen tekoon liittyy organisaation koko. Haastatteluissa kävi ilmi, että organisaation pieni koko voi viitata tietotaidon vähäisyyteen, jolloin organisaatiolla ei välttämättä ole mahdollisuutta etsiä ja raportoida käyttämiensä sovellusten ohjelmistovirheistä, vaan nämä organisaatiot nojaavat palveluntarjoajien tekemiin auditointeihin. Järjestelmillä voi kuitenkin olla automaattisia hälytysjärjestelmiä, jotka varoittavat, jos joltain tietyltä alueelta tai johonkin epätavalliseen aikaan ollaan yhteydessä organisaation palvelimiin.

Yksi haastateltavista neuvoi käyttämään kolmivaiheista riskienkartoitussuunnitelmaa: 1) Selvitä ensin kaikki tahot, jotka jollain tavalla pääsevät käsiksi yhtiön tietoliikenteeseen. 2) Kartoitetun käyttöhallintavastuiden kautta voidaan määrittää ne toimet, joita pitää suorittaa, jotta ulkoapäin tuleville uhille voitaisiin varautua. 3) Vaadi toimittajilta tiettyjä asioita, jotka tulee täyttää ennen, kun heidän kanssa tehdään sopimuksia. Lisäksi haastateltava sanoi, että tiettyihin toimittajiin voi liittyä maariskejä esimerkiksi tietokantojen tapauksessa (regulaatio estää datakeskuksien sijainnin tietyissä maissa).

”Hakkerit ovat sitten asia erikseen, joita varten on hankala varautua yksittäisenä organisaationa. Vastuu kaatuu hakkeritapauksissa IT-jättien harteille.”

Sisä- ja ulkoverkon tekninen tietoturvatarkistus

Eräs haastatelluista kertoi, että heidän sisä- ja ulkoverkkoon teetettiin tekninen tietoturvatarkastus organisaation itsensä toimesta. Samalla haastateltava sanoi, että he luottavat palveluntarjoajien kykyyn arvioida yleistä turvallisuutta. Esimerkiksi päätelaitteiden tietoturvallisuuden arvioinnin vastuu annetaan ulkoisille palveluntarjoajille. On huomioitavaa, että toinen haastatelluista organisaatioista kertoi heidän tutkivan myös isojen IT-jättien tekemiä sovelluksia (Applen sähköpostisovellus). Joten, tässäkin suhteessa organisaatiot eroavat jossain määrin kyvykkyyksien suhteen.

Yleisempää voi kuitenkin olla, että organisaatiot teettävät verkkojen tietoturvatarkistuksia ulkopuolisten yhtiöiden toimesta. ”Testimielessä saatetaan suorittaa hyökkäyksiä omaa verkkoa kohtaan. Tätä kautta voidaan löytää uhkia, joita ulkopuoliset voisivat hyödyntää. - - ”Niille, joille on tietoturvan johtamisen kypsyys korkealla, ja isommat resurssit (pörssiyhtiöt), niin nämä yhtiöt saattavat satunnaisesti tehdä verkkohyökkäyksiä omiin järjestelmiin. Ei nyt joka vuosi, mutta satunnaisesti. - - Tämä

voidaan toteuttaa työntekijän näkökulmasta tai sitten ihan ulkopuolelta", kertoi eräs haastatelluista. Lisäksi hän eritteli kyseisen toiminnan koskevan todennäköisimmin sellaisia aloja, joilla tietojen sensitiivisyydellä on suuri merkitys, esimerkiksi finanssi- ja pankkialalla näin on.

4.4 Ylin johto

Kriittisen tiedon tunnistaminen ja luokittelu

Kriittisen tiedon ja omaisuuden näkyvä luokittelu henkilöstön perspektiivistä tekee organisaation turvallisuuspolitiikasta ymmärrettävää ja konkreettista. Kriittisen tiedon näkyvä luokittelu voi myös parantaa organisaation turvallisuusasemaa, sillä henkilöstö näkee konkreettisia esimerkkejä kriittisestä tiedosta, ja oppii erottamaan eri turvallisuustason tietoja toisistaan. Haastateltavat kertoivat, että ylin johto tekee jossain määrin luokittelua kriittisen tiedon suhteen, riippuen organisaation koosta ja toimialasta. Tiedon sensitiivisyys ja bisneskriittisyys nousivat tärkeimmiksi syiksi luokitella tietoa esimerkiksi julkinen-sisäinen-salainen-asteikolla.
Eräs haastateltavista nosti työtehtäviin liittyvän asian vaikuttavan kriittisen tiedon luokitteluun. Hän sanoi, että esimerkiksi toimitusjohtajalla, HR-päälliköllä ja GDPR-asioista vastaavalla henkilöllä tulisi olla henkilökohtainen työkansio ja tulostin, joka ei saa olla yhteydessä verkkoon. Näiden positioiden tuottamat tiedostot ja tiedot tulisi turvata erityisellä varmuudella.

"Useimmiten ylin johto, HR ja hallitus ovat sellaisessa positiossa, joiden papereita tulee suojata."

Tietojen luottamuksellisuudesta huolehtiminen

Tietojen luottamuksellisuudella tarkoitetaan sitä, ettei ulkopuoliset pääse käsiksi salaisiin tietoihin. Aiheesta kysyttäessä haastateltavat olivat varsin yksimielisiä, sillä kaikki sanoivat, että hyvällä käyttövaltuushallinnalla on suuri merkitys luottamuksellisuudesta huolehtimisessa. Tällöin voidaan tietää, ketkä pääsevät mihinkin tiedostoihin käsiksi ja ketkä vastuussa tiedon vuotamisesta, jos sellainen tapahtuu. Riski jäädä kiinni pienentää luottamusaseman väärinkäyttöä.

Eräs haastateltavista sanoi, että IT:llä on iso rooli luottamuksellisuuden huolehtimisessa, sillä teknologiaratkaisut lopulta rajaavat väärien henkilöiden pääsyä salaisiin tietoihin. Lisäksi IT-osaston ja johdon välinen vuoropuhelu korostuu. Toinen haastateltavista kertoi, että sisäpiirilistojen ylläpitäminen voi auttaa luottamuksellisuudesta huolehtimisessa. Projektinimien käyttö ja tieto siitä, kuka näistä projekteista tietää, voi auttaa suojelemaan luottamuksellista tietoa.

Yksi haastateltavista kertoi: ”Käyttäytymisnormit ohjaavat toimintaa, mistä voi puhua. Ylin johto itse ymmärtää, että mistä asioista voi puhua ja mistä ei.” Eli huomattava merkitys luottamuksellisuudesta huolehtimiseen liittyy myös erilaisiin tapoihin toimia ja jaettuun ymmärrykseen siitä, mikä on hyvien tapojen mukaista toimintaa ja mikä ei. Hän lisäsi vielä, että yhtiön listaus vaikuttaa asiaan: arvopaperimarkkinalain vaatima tiedottaminen ja hiljainen aika voi aiheuttaa organisaation toiminnassa eroavaisuuksia.

”Listaamattomista yhtiöistä tiedon vuotaminen ei välttämättä aiheuta lain puolesta ongelmia, vaan se on enemmänkin operatiivisia ja asiakassuhteita haittaava asia.”

Tietojen eheydestä huolehtiminen

Tietojen eheydellä tarkoitetaan tiedon oikeellisuutta eli sitä, että tieto pysyy kaikkien eri osastojen välillä oikeana eikä se esimerkiksi vääristy missään vaiheessa. Eheydestä puhutaan esimerkiksi silloin, kun työntekijän tulisi ylläpitää masterdataa, ja hänen tulisi selvittää, onko tätä masterdataa ylläpitävässä tietokannassa tapahtunut muutoksia, jos hän ei ole itse tehnyt muutoksia siihen. Tällöin tärkeä kysymys on, miten työntekijä voisi varmentua täysin siitä, ettei datassa ole tapahtunut muutoksia. Kysymys on pääosin tekninen ja haastateltavat kertoivat, että eheyden ylläpitäminen on IT-osaston vastuulla.

Eräs haastateltavista sanoi: ”Johto on vastuussa tavoista ja normeista, miten tieto liikkuu ja pysyy eheänä organisaation sisällä.” Tämä ei kuitenkaan tarkoita sitä, että ylimmän johdon tulisi olla toteuttamassa niitä teknisiä ratkaisuja, joilla eheys ylläpidetään, vaan pikemminkin olla vaatimassa IT-johdolta asian ratkaisua. Toinen haastateltavista sanoi: ”Ylimmän johdon tehtävä on palkata sellainen henkilö tehtävään, joka pystyy hoitamaan tämän homman. - - Ylimmällä johdolla ei yleensä riitä osaaminen.”

”Ylin johto sanoo IT-pomolle, että hoida homma.”

Tietojen saatavuudesta huolehtiminen

Haastateltavat olivat yksimielisiä ylimmän johdon vastuusta asettaa ohjeistukset, vaatimukset ja tavoitteet tietojen saatavuudesta sellaisiksi, että IT-johto voi toteuttaa nämä omassa työssään. Tällöin voidaan sanoa, että ylin johto on vastuussa oleva (accountable) ja IT-johto vastuullinen (responsible). ”Ylimmän johdon tulee tietää, että ennalta määrätyssä ajassa järjestelmät saadaan ylös ja tiedot palautettua”, kuten eräs haastateltavista kuvasi johdon vastuiksi. Lisäksi haastatteluista selvisi, että ylimmän johdon tulee olla tietoinen järjestelmien palautumiskyvystä ja kommunikoida näistä muulle organisaatiolle.

”Ylin johto huolehtii tästä asiasta niin, että se palkkaa sinne sellaisen IT-johdon, joka osaa hoitaa homman ja määritellä nämä asiat.”

Organisaation jatkuvuudesta huolehtiminen

Eräs haastateltavista sanoi, että ylimmällä johdolla on suuri vastuu huolehtia organisaation jatkuvuudesta, sillä kaikkien toimintojen tulisi tähdätä toimintojen jatkuvuuteen. Hän kertoi toisaalta, että IT-osaston vastuulle kuuluu jatkuvuussuunnitelmien teko, kriittisyysluokittelu ja niistä raportoiminen. Hän sanoi myös: ”Ylimmän johdon tulisi edellyttää testausta ja harjoittelua. Testata sitä, että toimiiko suunnitelmat.”

Toinen haastateltavista sanoi, että IT-johdon vastuulla on kertoa ylimmälle johdolle ymmärrettävästi, että tällä tavalla meidän organisaatiossa tämä asia hoidetaan. Hän kertoi myös, että jatkuvuus- ja varautumissuunnittelulla on hyvin merkittävä vaikutus organisaation toimintojen jatkuvuudessa.

” - - Joillakin tehtailla on tapahtunut tulipaloja, mutta näihin liittyvät haaverit on onnistuttu minimoida hyvien käytäntöjen ja varautumissuunnitelman ansiosta. Koulutus on tällöin avainasemassa, ja sen varmistaminen, että ihmiset tietävät, miten toimia näissä tilanteissa.”

Toipumissuunnittelu ja toimintojen jatkuvuuden turvaaminen

Toipumissuunnittelu pyrkii vastaamaan mahdollisiin tietoturvauhkiin ja tämän suunnittelun tekeminen on IT-osaston vastuulla, joka pohjautuu ylimmän johdon asettamiin tavoitteisiin. Se voisi olla esimerkiksi ”top5/top10 tietoturvauhkaa, ja näihin vastaaminen ja arviointi. - - Raportointi muulle organisaatiolle, kun uhka on havaittu”, kuten eräs haastateltavista kiteytti.

Toinen haastateltavista kertoi, että toipumissuunnitelman toteuttamisesta ei sellaisenaan kerrota ylimmälle johdolle todennäköisen tietotaidon puutteen takia. Toipumissuunnitelma pidetään IT-osaston sisällä ja siitä viestitään ymmärrettävästi ylimmälle johdolle. ”Liiketoimintayksiköiden sisällä todennäköisesti näihin on varauduttu. Riskienhallintajohto on näistä vastuussa.”

”Kaksi asiaa, joiden välillä tasapainoillaan: aika ja raha. Riippuen kuinka nopeasti organisaatio haluaa järjestelmät takaisin ylös, niin tätä voidaan mitata rahalla.”

Nykyisten kontrollien arviointi

Nykyisten kontrollien toimivuutta tulee arvioida, jotta ylimmällä johdolla olisi paras tieto nykyisten prosessien toimivuudesta. Lisäksi kontrollien arvioinnilla voidaan pyrkiä nostamaan organisaation turvallisuustasoa tekemällä jotkin prosessit läpinäkyvämmiksi, joissa kontrolleilla on suuri vaikutus. Nykyisten kontrollien arvioinnilla ylin johto voi myös saada selville, miten kontrolleja tulisi tulevaisuudessa asettaa. Näistä lisää seuraavassa kappaleessa.

Eräs haastateltavista kertoi, että heidän organisaatiossa kontrollien toimivuutta arvioidaan jälkikäteistarkastuksilla, esimerkiksi lokeilla sekä käyttöoikeuksien avulla rajataan virheiden teon riskiä. Heillä ei ilmeisesti ole ennaltaehkäisevää toimintaa, josta muut haastateltavat mainitsivat. Ennaltaehkäisevää toimintaa voisi esimerkiksi olla sisäisen tarkastajan käyttäminen säännönmukaisin väliajoin. Yksi haastateltavista kertoi: ”Tärkeään roolin asettuu sisäinen tarkastus, joka voi omissa kontrollitesteissään löytää jotakin huomioitavaa. Ylimmän johdon vastuulla on reagoida näihin löydöksiin.”

Toinen haastateltava kertoi oman näkemyksen kontrollien asettamisen vastuisiin: ”Ylimmällä johdolla ei ole kyvykkyyksiä vastata näihin kysymyksiin, vaan näistä vastaa tietohallintojohtaja.” Tässä on ilmeisesti tarkoitettu, että tietohallintojohtaja vastaa kontrollien mekaanisesta asettamisesta, mutta ylin johto sitten päättää lopulta, että millä tavalla kontrolleja tulisi asettaa liiketoiminnan näkökulmasta.

Uusien kontrollien asettaminen

Uusia kontrolleja asetetaan yhden haastateltavan mukaan: ”Hyväksymällä uusia politiikkoja ja toimintamalleja. Rakentamalla sopivan organisaation eri toimintoihin. Lisäksi organisaation tehtävänä on miettiä yksittäisiä prosesseja ja niiden ongelmakohtia ja kontrolleja. Näiden rakenteiden kautta ylin johto asettaa kontrolleja.” Voisi sanoa, että alemmille tasoille annetaan yleiset suuntaviivat, joiden mukaan tulisi toimia, jonka jälkeen alemmalta tasolta raportoidaan ylimpään johtoon epäkohdista ja puutteista. Näin luuppi sulkeutuu.

Toinen haastateltavista sanoo, että kontrollien asettaminen pitäisi lähteä toiminnallisesta lähtökohdasta ja perustua järkevyyteen: kannattaako tällaisia kontrolleja ylipäätään asettaa kyseiseen asiaan? Sillä ei kannata tehdä tietoturvaa tai asettaa kontrolleja, jotta olisi tietoturvaa ja kontrolleja; vaan näitä pitäisi pohtia liiketoimintojen kautta. Hän jatkaa: ”Jos ylin johto miettisi, miten kontrolleja tulisi asettaa, tällöin heidän työaikansa menisi ihan väärään asiaan.”

”IT-johdon vastuulla on päättää tietoturva-asioista, ja viestiä nämä ylimmälle johdolle selkeällä ja ymmärrettävällä tavalla.”

5 Keskustelu

5.1 Tilivelvollinen (accountable) vai vastuussa oleva (responsible)?

Teoreettista pohdintaa

Vastuullisessa asemassa oleva ihminen on loppukädessä vastuussa kyseiseen työtehtävään/toimintaan liittyvistä oikeudellisista ja toiminnallisista vastuista. Tämä tarkoittaa, että organisaation toimitusjohtaja on vastuullinen kaikesta organisaatioon liittyvästä toiminnasta, vaikka hän ei itse suorittaisi kaikkia näitä toimintoja. Esimerkiksi projektipäällikkö tekee suurimman osan omaan projektiin liittyvistä päätöksistä, ja on tätä kautta vastuussa oman projektin kannattavuudesta ja raportoinnista. Harvemmin mediassa näkee kuitenkaan esimerkissä kuvatun projektipäällikön puolustavan omaa projektiaan käräjillä, jos lakia ei ole noudatettu. Käräjillä organisaatiota usein puolustaa lakimies, joka on todennäköisesti valittu ylimmän johdon toimesta, jonka valinnasta loppupeleissä on vastuussa toimitusjohtaja.

Toimitusjohtajaesimerkki kuvastaa sitä, miten toimintaan liittyvä työntekijä (projektipäällikkö tai lakimies) suorittaa omaa työtehtävää vastuullisen henkilön puolesta, joka tässä on toimitusjohtaja. Lisäksi voidaan sanoa, että projektipäällikkö ja lakimies ovat vastuussa tekemisistään käräjöinnin suhteen, sillä he ovat olleet myötävaikuttamassa organisaation toimintaan ja he ovat olleet johdattamassa organisaatiota käräjöinnin suhteen johonkin lopputulokseen. Vastuullinen on viime kädessä vastuussa käräjäoikeuden päätöksestä.

Tutkimustulosten yhteensopivuus teoreettisen pohdinnan kanssa

Haastatteluiden aikana havaittiin, että vastuunmäärittely eri asioiden suhteen oli vahvasti kiinni haastateltavan omasta roolista/työtehtävästä. Kappaleessa 4.4, kohdassa ”Tietojen eheydestä huolehtiminen”, havaittiin eroavaisuutta vastuumäärittelyn suhteen: eräs haastateltavista esimerkiksi sanoi, että IT-osasto on vastuullinen eheydestä huolehtimisessa, kun taas prosessi- ja systeemikonsultti sanoi ylimmän johdon olevan vastuussa tästä asiasta. Ristiriita haastateltavien ja teorian välillä, voi viestiä siitä, ettei kyseinen taho välttämättä ole ymmärtänyt tilivelvollisuuden ja vastuussa oleva-käsitteiden

eroavaisuutta. Lisäksi voidaan todeta, että suomen kielestä ei löydy englannin kielen vastaavia ilmauksia (accountability/responsibility), jolloin vastuullisuus-käsitteen syvällinen ymmärtäminen voi jäädä pintapuoliseksi.

Tutkimuksen rajallisuuden takia on haastavaa sanoa, johtuuko eroavaisuudet vastuumäärittelyssä teoreettisen ja käytännön maailman kohtaanto-ongelmasta, jolloin yritysmaailmassa toimivat ihmiset ovat vieraantuneet teoreettisen maailman asioista eikä asioita enää osata katsoa teoreettisen viitekehyksen silmin. Joka tapauksessa tutkimustulokset viittaavat siihen, että vastuukäsityksien pohtiminen ei ole ylimmän johdon ja joidenkin konsulttien jokapäiväisen pohdinnan keskiössä.

5.2 IT:tä koskevat investoinnit & päätöksenteko

IT-investoinnit teoreettisesta näkökulmasta

IT:tä, kuten kaikkia muitakin toimintoja koskevat investoinnit tulisi evaluoida jonkin systemaattisen tavan avulla. Tulisi esimerkiksi määrittää etukäteen, mihin tavoitteisiin investoinnilla pyritään ja millä tavalla investointi voisi esimerkiksi tehostaa organisaation toimintaa. Tämän jälkeen evaluoinnissa tulisi selvittää määrällisesti mitattavat hyödyt ja mahdolliset aineettomat hyödyt, joita investoinnilta voidaan odottaa. Lopulta, investoinnin koosta riippuen, hallitus hyväksyy tai hylkää investoinnin, jota toimiva johto alkaa toteuttaa (Ward, ym. 2008).

IT-investointeja koskevaa päätöksentekoprosessia voidaan myös lähestyä investoinnin pakollisuuden näkökulmasta, jolloin investointeja harkitaan eri tavoilla niiden luonteesta riippuen (Joshi & Pant, 2008). Esimerkiksi GDPR-asetusta koskeva lainsäädäntö käytännössä pakotti organisaatiot investoimaan omiin tietojärjestelmiin, eikä tällöin Joshi'n & Pant'n (2008) mukaan ole järkevää käyttää johdon aikaa määrittämään investoinnin ROI:ta tai NPV:tä, vaan johdon tulisi optimoida oma aikansa kustannustehokkaiden järjestelmien etsimiseen ja hankkimiseen.

Tutkimustulosten yhteensopivuus teorian kanssa

IT-asioita koskeva päätöksenteko: Tutkimustulokset viittaava siihen, että nykyään IT-investointeja tehdään yhä enemmän liiketoimintojen ehdoilla, sillä aloitteet uusista hankkeista tulevat liiketoiminnoista vastaavissa yksiköissä. IT-osaston tehtäväksi jää konsultatiivinen ja toimeenpaneva rooli, joka

vastaa hankkeen integraatiosta organisaation järjestelmiin. Lisäksi havaittiin, että organisaation koko vaikuttaa IT-investointien päätöksentekoon. Isoimmissa organisaatioissa IT-asioista päätöksiä tehdään isommissa tiimeissä, kun taas pienemmissä organisaatioissa päätökset voivat olla yhden tai kahden henkilön tekemiä, kuten eräs haastateltavista kertoi. Tällöin vastuu parhaiden IT-järjestelmien hankinnasta voi pahimmassa tapauksessa vaarantua, jos johto on esimerkiksi epäonnistunut IT-asioista päättävien ihmisten rekrytoinnissa. Päinvastoin, pienessä organisaatiossa päätökset todennäköisemmin voidaan tehdä tehokkaammin johtuen keskittyneemmästä päätöksenteosta.

IT-hankintojen prosessikuvaus: Todennäköisesti haastateltavien roolien ja näiden organisaatioiden vallitsevien käytäntöjen takia, varsinaista ylimmän johdon päätöksentekoprosessia ei juurikaan haastatteluiden avulla saatu selville. Tätä kuvastaa haastatteluiden pohjalta koostettu **kuvio** ” IT-hankintojen prosessikuvaus”-kohdassa, jossa ei käytännössä mainittu ollenkaan ylimmän johdon osallistumista IT-hankintoja koskeviin päätöksiin. Luultavasti paras selitys tälle on hyvä hallinnointitapa: hallitus ja toimiva johto haluavat antaa liiketoiminnoista vastaaville yksiköille tilaa keskittyä parhaalla mahdollisella tavalla bisneksen kehittämiseen, ja sen takia näitä ei juurikaan mainittu haastateltavien toimesta.

Joshi & Pant (2008) kertovat omassa tutkimuksessaan, että hallituksen rooli IT-investoinneissa on puhtaasti taloudellinen ja strateginen. Jos esimerkiksi koetaan, että uutta IT-järjestelmää koskeva hankinta on riittävän iso ja strateginen, hallituksen rooli todennäköisesti korostuu päätöksenteossa. Tutkimustuloksista ei todennäköisesti sen takia löydetty Joshi’n & Pant’n (2008) tutkimuksen mukaista tulosta, koska haastateltavat luultavasti näkivät käytännön työn (operatiivinen yksikkö tekee aloitteen ja IT-osasto konsultoi ja valvoo) olevan etusijalla järjestelmähankkeissa. NPV- ja ROI-laskelmat ovat kuitenkin loppujen lopuksi vain mekaanisia laskutoimituksia, kun tärkeämpää varsinkin IT-järjestelmähankkeissa olisi harkita työntekijöiden kokemaa lisäarvoa (esimerkiksi työn mielekkyyttä lisäävät komponentit ja aiempaa joustavampi työnkuva).

Lisätöiden hyväksyminen IT-hankkeisiin: Tutkimustuloksista havaittiin, että IT-hankintojen toimeenpanon aikana tapahtuvilla toimenpiteillä on vaikutusta lopulliseen järjestelmään. Esimerkiksi hankintayksikkö ja ohjausryhmä voi havaita, että alun perin asetetut tavoitteet eivät vastaa organisaation todellisia vaatimuksia, jolloin tarpeita joudutaan määrittelemään uudelleen. Haastateltavat kertoivat, että IT-hankintoja suunniteltaessa hankintayksikön tulisi selvittää mahdollisista lisätöistä aiheutuvat kustannukset jo etukäteen. Lisäksi hankkeeseen osaaottavien ihmisten sitouttaminen havaittiin tärkeänä asiana hankkeen läpiviennin kannalta.

Ihmisten sitouttaminen ja tehokkaan ohjausryhmän toiminta rakentuvat lähtökohtaisesti hyvän kommunikaation varaan. Tutkimustuloksista havaittiin, että kommunikaation merkitys nostettiin esille yhä uudelleen ja uudelleen IT-hankkeita toimeenpanevassa keskustelussa.

Tietoturvan varmistaminen järjestelmähankkeissa: Tutkimustulokset antavat viitteitä ulkoisen palveluntarjoajan osallistamisen kannattavuudesta järjestelmähankkeiden suunnitteluun ja käyttöönottoon. Haastateltavat kertoivat, että sillä ei välttämättä ole mitään merkitystä tietääkö hankkiva liiketoimintayksikkö millainen järjestelmä toimisi parhaiten, jos näistä tarpeista ei osata viestiä oman IT-osaston kanssa, saatikka IT-järjestelmiä toimittavan organisaation kanssa. Haastateltavat kertoivat, että järjestelmätoimittaja tulee ottaa mukaan jo suunnitteluvaiheessa mukaan prosessiin, jotta järjestelmätoimittaja voisi kertoa niistä toiminnoista, jotka pystytään toimittaa normaalien ehtojen mukaan. Lisäksi järjestelmätoimittaja voi kertoa mahdollisista lisätoiminnoista, joita käsiteltäisiin erillisinä sopimuksina. Tällöin hankkeen hallinta helpottuu organisaation ja sitä toimittavan organisaation näkökulmasta, sillä normaalien ehtojen mukaan toimitettava sisältää perusjärjestelmärungon, jonka päälle rakennetaan halutut lisätoiminnot.

Toiseksi tärkein asia järjestelmähankkeita koskevassa keskustelussa oli auditointien tekeminen meneillään olevaan järjestelmähankkeeseen sekä auditointien kautta nousevat tarpeiden uudelleen määrittelyt. Näistä ensimmäinen tarkoittaa esimerkiksi sitä, että hankkiva organisaatio palkkaa ulkoisen kyberturvayhtiön tekemään auditoinnin hankittavan järjestelmän tietoturvasta ja joka raportoi havaituista puutteista, jonka jälkeen alkuperäiset tarpeet voidaan määrittää uudelleen vastaamaan paremmin haluttua lopputulosta. Haastateltavat kertoivat myös, että on tavallista, että organisaatiot tekevät omia auditointeja meneillään olevaan hankkeeseen. He kertoivat, että on todennäköisempää saavuttaa haluttu lopputulos, jos järjestelmähanketta ohjataan proaktiivisesti jo sen toteuttamisvaiheessa eikä vasta luovutusvaiheessa.

Liiketoimintayksiköiden välillä tapahtuva tiedon välitys: Joskus investointihankkeet koskevat useampaa liiketoimintayksikköä, jolloin vastuiden, velvollisuuksien sekä käyttöoikeuksien määrittelystä voi tulla haastavaa järjestelmän näkökulmasta. Lisäksi tulee selvittää mahdollisten vaarallisten työyhdistelmien syntyminen. Joskus vaarallisista työyhdistelmistä ei päästä eroon, jolloin ainoa tapa on ensinnäkin tiedostaa nämä järjestelmään liittyvät uhat ja sitten vastata näihin uhkiin.

Tutkimustuloksista ilmeni, että yksi tapa ratkaista edellä mainittuja uhkia on RACI-mallin luominen, jossa ristiintaulukoidaan eri työtehtäviin liittyvät vastuut ja velvollisuudet, jolloin RACI-malli tuo konkreettisesti näkyville, kuka mihinkin työtehtävään osallistuu ja mitkä ovat tiettyyn työtehtävään

liittyvien eri ihmisten velvollisuudet. Mallilla voidaan erään haastateltavan mukaan vastata tehokkaasti mahdollisiin uhkiin, joita organisaatiorakenteeseen voisi liittyä.

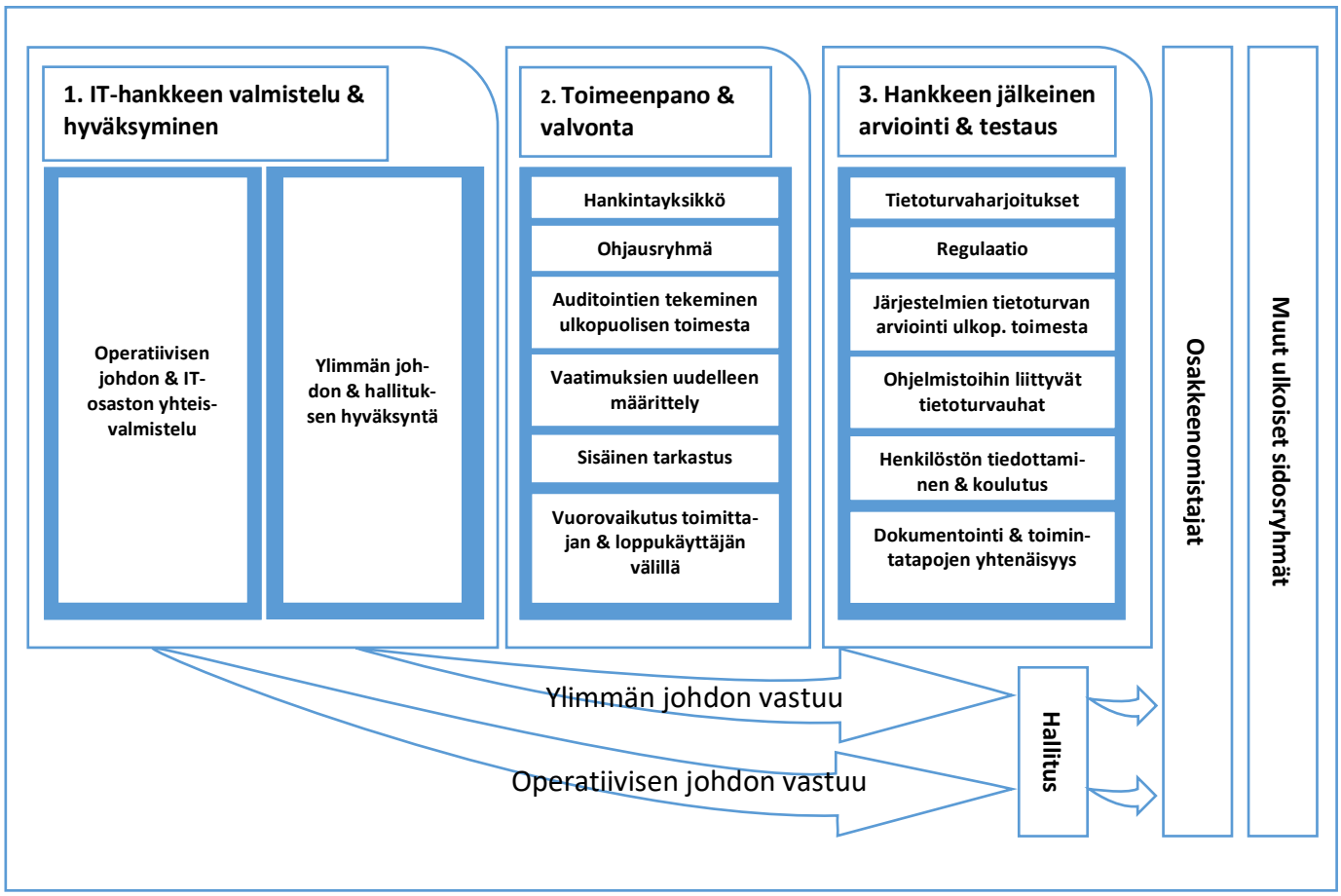
Lisäksi tutkimustuloksista ilmeni, että RACI-mallia voidaan käyttää investointiprosessin aikana esimerkiksi ohjausryhmän avustavana työkaluna, jossa selvitetään IT-hankkeeseen osaaottavien ihmisten välisiä vuorovaikutussuhteita. Konkreettisesti tämä voisi tarkoittaa järjestelmän loppukäyttäjän ja järjestelmää ohjelmoivan insinöörin kohtaamista, jossa loppukäyttäjä informoi insinööriä omasta työnkuvastaan. Tällöin insinöörille syntyy parempi kuva halutusta lopputuloksesta, jolloin IT-hankinnan näkökulmasta voidaan saavuttaa parempi lopputulos. Lisäksi keskusteluun voitaisiin ottaa projektipäällikköjen ja yksikön johtajan mielipiteet vastuista sekä käyttöoikeuksista. Eräs haastateltava kertoi, että tämänkaltainen RACI-mallin käyttö investointihankkeen aikana on käytännössä ainoa tapa onnistua investoinnin toteuttamisessa läpinäkyvästi ja luotettavasti. Isojen investointien kohdalla tämä näkemys vain korostuu.

6 Yhteenveto

6.1 Tutkimuksen yhteenveto

Tutkimuksen yhteenvetona esitetään **Kuvio 3**, jossa on kuvattu haastatteluissa havaittuja asioita IT-hankkeen näkökulmasta. Tämä valinta tehtiin, sillä haasteltavien organisaatioiden liiketoiminta perustuu erilaisille projekteille, joissa käytetään valtaa ja tehdään päätöksiä eri asioista. Itsessään valta ja vastuu näkyvät ihmisten välisissä suhteissa, joka on abstraktia ja vaikeasti selitettävää. Tämän takia yhteenvedossa on pyritty abstraktoimaan valta- ja vastuukysymykset, ja tuoda nämä konseptit helpommin ymmärrettävään muotoon. Projektimalli on tästä syystä valittu kuvaamaan eri toimijoiden välisiä vastuu- ja valtarakenteita, sillä ihmiset ottavat projektien aikana erilaisia rooleja ja vastuuseen ja päätöksentekoon liittyen (ks. RACI-malli kappaleessa 4.2). Tällöin on epäselvää, kenen aloitteesta mikäkin asia on saanut alkunsa, ja ainoastaan on selvää, kuka viime kädessä kantaa vastuun projektin onnistumisesta tai epäonnistumisesta.

Kuviossa esitellään tutkimuksen kannalta keskeisimmät aiheet: 1) kuka on vastuussa organisaation tietoturva-asioista; ja 2) miten hallitus ja ylin johto suhtautuvat organisaation tietoturvaan. Kuvio on jaotellut IT-hankkeen läpikäymät vaiheet ja näihin vaiheisiin liittyvät keskeisimmät toimijat. Tietyn vaiheen toimijoiden keskinäinen suhde ei ole määritelty, mutta nämä toimijat pyrkivät omalla menettelyllään edistämään IT-hankkeen tavoitteita niin liiketoiminnan kuin tietoturvan näkökulmasta. Kuvion alle on kerätty lyhyt kuvaus jokaisesta toimijasta niin itse projektissa kuin toimijan vaikutus organisaation tietoturvaan.



Kuvio 3: IT-hankkeen elinkaari & eri toimijoiden ja konseptien suhteet hankkeen aikana.

1. IT-hankkeen valmistelu & hyväksyminen

- **Operatiivisen johdon & IT-osaston yhteisvalmistelu**: Operatiivinen yksikkö tekee aloitteen ja kertoo omista tarpeistaan IT-osastolle. IT-osasto auttaa aloitteen valmistelussa ja määrittelee IT-vaatimukset. Hyvin tarkka määrittely vastuista: mistä kaikesta palveluntarjoaja vastaa esimerkiksi tietovuodon tapauksessa. IT-tiimi määrittelee hyväksyttävät riskit tietoturvan suhteen, jotka ylin johto hyväksyy.
- **Ylimmän johdon & hallituksen hyväksyntä**: Hanke voi vaatia vielä hallituksen hyväksynnän, jos hanke on organisaation näkökulmasta strateginen. Hallitus tekee lisäselvityksiä hyödyistä/haitoista, ja tekee lopullisen päätöksen hankkeen käynnistämisestä. Kun hanke käynnistetään, hallituksen tilivelvollisuus alkaa.

2. Toimeenpano & valvonta

- **Hankintayksikkö**: Operatiivisen yksikön alle perustetaan hankintayksikkö, jonka rooli on puhtaasti neuvotteleva ja taloudellinen.
- **Ohjausryhmä**: Perustetaan ohjausryhmä, joka valvoo hankkeen etenemistä: mitä töitä on tehty ja mitä tullaan vielä tekemään.
- **Auditointien tekeminen ulkopuolisen toimesta**: Hankkeen edetessä palkataan ulkopuolinen organisaatio tekemään auditointeja.
- **Vaatimuksien uudelleen määrittely**: Auditointiraporttien avulla vaatimuksia voidaan määritellä uudelleen.
- **Sisäinen tarkastus**: Organisaation sisällä voidaan toteuttaa sisäistä tarkastusta, johon voidaan käyttää RACI-mallia.
- **Vuorovaikutus toimittajan & loppukäyttäjän välillä**: Tehdään pilottikokeiluita palveluntarjoajan kanssa parhaan ratkaisun löytämiseksi. Ohjelmistokehittäjän ja loppukäyttäjän vuorovaikutus on tärkeää.

3. Hankkeen jälkeinen arviointi & testaus

- **Tietoturvaharjoitukset**: Tietoturvaharjoituksien säännöllinen järjestäminen. Testataan organisaation kykyä vastata tietoturvauhkiin.
- **Regulaatio**: Regulaatio saattaa asettaa uusia vaatimuksia organisaatiolle ja näiden tiedonkäsittelylle. Esimerkiksi GDPR-asetus.
- **Järjestelmän tietoturvan arviointi ulkopuolisen toimesta**: Palkataan ulkopuolinen kyberturvayhtiö määrittelemään organisaation tietoturvan tasoa. Ulkopuolista voidaan pyytää murtautumaan organisaation järjestelmään, jolloin mahdolliset haavoittuvuudet voidaan löytää.
- **Ohjelmistoihin liittyvät tietoturvauhat**: Ohjelmistokehittäjät ilmoittavat ohjelmistoihin ja järjestelmiin liittyvistä uhista. Organisaation tulee pystyä mukautumaan mahdollisiin organisaation muutoksiin.
- **Henkilöstön tiedottaminen & koulutus**: Pidetään henkilöstö ajan tasalla mahdollisista tietoturvauhista. Pyritään proaktiiviseen toimintaan.

- **Dokumentointi & toimintatapojen yhtenäisyys**: Dokumentoidaan työtehtävät niin, että kuka tahansa pystyisi hoitaa kyseistä tehtävää. Periaatteiden, politiikkojen ja toimintatapojen viestintä henkilöstölle.

Operatiivisen & ylimmän johdon vastuut

- **Operatiivinen johto on vastuullisessa asemassa**: Liiketoimintajohtaja sekä IT-osasto ovat vastuullisessa asemassa, jotka raportoivat toimitusjohtajalle ja hallitukselle näiden tekemien selvitysten mukaan.
- **Hallitus on tilivelvollinen osakkeenomistajia & muita sidosryhmiä kohtaan**: Tilivelvollisuus lankeaa lopulta hallituksen harteille, kun osakkeenomistajat arvioivat hallituksen toimintaa yhtiökokouksessa osakeyhtiölain 1.luvun 5§:n mukaan.

6.2 Käytännön merkitys

Käytännön vinkkejä haastatteluista

Pyri aina miettimään liiketoiminnan etua – teknologinen ratkaisu ei aina ole paras mahdollinen: Kynä ja paperi voi olla jossain tilanteissa edelleen paras muistiinpanojen tekomuoto – ja tämä pätee myös moniin muihinkin asioihin. Liiketoimintaa ei tulisi tehdä teknologia edellä, vaan liiketoiminta edellä.

Punnitse tietoturva- ja IT-hankinnat käytännön, turvallisuuden ja investoinnin monetaarisesta näkökulmista: Voit saada tehokkaan, työntekijöiden työtä helpottavan ja tietoturvallisen järjestelmän, mutta et halpaa järjestelmää samanaikaisesti. Saat valita näistä kaksi asiaa – kolmas tulee annettuna kahden valitun asian suhteena.

Vuorovaikutus IT-johdon ja operatiivisen johdon välillä: IT-osasto ei aina ymmärrä alla olevaa liiketoimintaa täysin, eikä operatiivinen johto myöskään aina ymmärrä IT-osaston työtä. IT-osaston tulisi liikkua lähemmäs liiketoimintayksikön toimintaa, jotta se voisi tehdä parempia päätöksiä liiketoiminnan näkökulmasta. Myös liiketoimintajohtajan tulee ymmärtää IT-osaston työtä, jotta se osaisi ottaa tietoturvauhat huomioon omassa työssään.

Tietoturvaharjoituksien järjestämisen ottaminen osaksi henkilöstön kouluttamista: Näitä järjestetään yhä liian harvoin, jos ollenkaan. Hakkereista ja tietoturvaa uhkaavista sovelluksista tulee koko ajan fiksumpia ja ainoa tapa vähentää uhkien konkretisoitumasta on pitää henkilöstö koulutettuina. Näin ihmiset hahmottaisivat paremmin myös omaan arkeen liittyviä tietoturvauhkia. Liitteessä yksi näistä arkeen liittyvistä uhista on kirjoitettu lisää.

Pyri ymmärtämään ja hyväksymään tietyt tietoturvariskit – ulkopuolinen kyberturvayhtiö auttaa tässä: Kaikkeen tietoverkoissa tapahtuvaan toimintaan liittyy riskejä, ja tänään jokin pomminvarma tietoturva-asia voi vuoden päästä olla jo vanhentunut. Tästä syystä tietoturvauhat pitää selvittää, ne pitää ymmärtää ja niihin pitää varautua. Myöskin ne pitää hyväksyä, jotta toimintaa voitaisiin jatkaa.

6.3 Tutkimuksen rajallisuus

Vakuutusyhtiöiden näkökulma

Tutkimuksessa ei kysytty vakuutusyhtiöiden tai vakuutusmeklareiden näkökulmaa tutkittuun ilmiöön, sillä vakuutusyhtiöt eivät kuuluneet alkuperäiseen tutkimussuunnitelmaan. Monet haastateltavista olivat sitä mieltä, että vakuutuksia myyvien tahojen haastattelu olisi saattanut tuoda jonkin uuden näkökulman tutkittuun ilmiöön. Vakuutuksia myyvissä yhtiöissä nimenomaan keskitytään määrittelemään erilaisia vastuita ja velvollisuuksia jonkin tietyn onnettomuuden tai uhan konkretisoituessa.

Voidaan sanoa, että vakuutusyhtiöiden haastattelu olisi voinut tuoda jonkin uuden näkökulman tutkittuun aiheeseen, mutta haastatteluasetelmaa oltaisiin todennäköisesti jouduttu muuttamaan sen verran, ettei se olisi enää muistuttanut alkuperäistä, eli Dutta'n & McCrohan'n (2002) esittelemää viitekehystä. Tästä syystä vakuutusyhtiöiden haastatteluiden sisällyttäminen tutkimukseen voisi olla seuraavan samaa aihetta tutkivan pro gradu-tutkielman lähtökohta.

Suurempi otanta

Tämän tutkimuksen haasteena oli teoreettisen viitekehyksen muuttaminen käytännön maailmaan, mikä osaltaan vaikutti haastateltavien määrään (5). Tutkimusta olisi voitu jatkaa haastattelemalla useamman alan edustajia, jotta oltaisiin voitu saada parempi näkökulma ylimmän johdon vastuu-käsityksistä. Lisäksi **Tutkimuksen yhteenveto**-kappaleessa esitellyn kuvion 2. vaihetta olisi voitu tutkia laaja-alaisemmin ja tarkemmin. Oltaisiin esimerkiksi voitu selvittää, miten hankintayksikön ja operatiivisen johdon vuorovaikutusta hoidetaan IT-hankkeen aikana; miten vaatimuksia määritellään uudellaan; ja miten kuvion eri muutokset vaikuttavat lopulliseen IT-järjestelmään.

Tutkimuksen syvyydestä ja laajuudesta on kirjoitettu jo kappaleessa **3.2**, jonka alaotsikko *Tutkimuksen laajuus & syvyys* kertoo lisää tutkimuksen otantajoukosta.

6.4 Tutkimuksen pohjalta syntyneet tutkimuskohteet

Vakuutusyhtiöiden/vakuutusmeklarien näkökulma kyberturva-asioiden vastuista

Tämän tutkimuksen haastatteluvaiheessa havaittiin, että haastateltavat organisaatiot pohtivat omien ja muiden organisaatioiden varautumista mahdollisiin tietovuotoihin, ja miten tietovuotoihin sisältyviä riskejä voitaisiin rajata esimerkiksi vakuutuksien avulla. Yleisesti järjestelmätoimittaja ja järjestelmän hankkija sopivat yhdessä kannetuista vastuista, ja siitä miten esimerkiksi vahingonkorvausvastuut jakautuvat rikkomustilanteessa. Uuden näkökulman näiden kahden entiteetin vastuiden jakautumiseen voisi tuoda vakuutusyhtiöiden tarjoamat kyberturvavakuutukset.

Todennäköisesti vakuutusyhtiöt vaativat organisaation tietojärjestelmiltä tiettyjä sertifikaatteja ennen vakuutuksien myöntämistä, sillä tietojärjestelmiin liittyvää teknologiaa saattaisi muuten olla haastavaa määritellä standardoidusti. Tästä syystä tutkija voisi pyrkiä hahmottamaan mahdollista haastatteluasetelmaa yhdessä vakuutusyhtiön/-meklarin kanssa, jolloin tutkija voisi ymmärtää paremmin vakuutusmaailmaan liittyviä lainalaisuuksia. Samalla tutkija voisi tuoda keskusteluun teoreettisen näkemyksen vastuista ja velvollisuuksista. Lisäksi tutkija voisi käyttää apuna tässä tutkimuksessa käytettyjä aihealueita, joita esimerkiksi ovat: varautumissuunnittelu, tietoturvan varmistaminen järjestelmähankkeissa ja tietoturvan huomiointi ulkoistuksissa.

Kyberturva-asioiden toteuttaminen ja niiden arviointi vaativat paljon teknistä osaamista tietojärjestelmistä ja organisaation ylätason toiminnasta, ja sen takia voisi olla mielekästä haastatella IT-konsultteja, riskienhallinta-ammattilaisia sekä vakuutusyhtiöiden omia tietojärjestelmäammattilaisia (, jotka olisivat perehtyneet mahdollista vakuutusta hakevien organisaatioiden järjestelmiin).

Organisaation tietoturvatason määrittely – onko yhtiön tietoturva halutulla tasolla

Tämän tutkimuksen alkuperäinen suunnitelma oli tutkia organisaatioiden tietoturvan tasoa ja vastata hyvin yksiselitteisesti kysymykseen: ”Onko organisaation tietoturva halutulla tasolla?” Tämänkaltaisessa tutkimusasetelmassa tultiin hyvin nopeasti havaittua, ettei organisaatioiden tietoturvaa voida arvioida näin yksinkertaisella kysymyksellä, vaan organisaatioiden tietoturva on paljon muutakin kuin vain tietojärjestelmiä ja palomuureja.

Tämän tutkimuksen pohjalta voitaisiin tehdä jatkotutkimusta organisaatioiden tietoturvan tasosta, ja pyrkiä vastaamaan, onko organisaation tietoturva ylimmän johdon asettamalla tasolla. Tässä tutkimuksessa on puhuttu varautumissuunnitelmasta, erilaisista teknologisista ratkaisuista tietoturvan parantamiseksi ja ihmisten kouluttamisesta. Jokainen näistä on merkittävä tekijä organisaation tietoturvan tason kannalta, ja näitä voitaisiin mahdollisesti pohtia seuraavassa tutkimuksessa.

Haastateltaviksi organisaatioiksi voitaisiin ottaa isompia organisaatioita, joilla on jo standardoidut tavat toimia ja valmistella uusia hankkeita. Ensinnäkin tutkija voisi löytää konsensuksen isompia organisaatioita tutkiessa, ja toiseksi, määritellä tätä kautta uutta teoriaa parhaista prosesseista, joita tulee ottaa huomioon tietoturvan tasoa määriteltäessä.

7 Lähteet

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2015), ”Tietosuojakäsikirja johdolle”, *Tietosanoma Helsinki.*

Anderson, R. (1996), “From critics to coaches”, *Bank Management;* 72, pp. 26-32.

Dutta, A. & McCrohan, K. (2002), ”Management's Role in Information Security in a Cyber Economy”, *California Management Review,* Vol. 45, NO.1.

Herath, T. & Rao, H. (2009), “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness”, *Decision Support Systems,* 47, pp. 154-165.

Holopainen, J., Koivu, E., Kuuluvainen, A., Lappalainen, K., Leppiniemi, J., Mikola, M. & Vehmas, K. (2013), ”Sisäinen tarkastus”, *Tietosanoma Helsinki*.

Joshi, K. & Pant, S. (2008), ”Development of a Framework to Asses and Guide IT Investments: An Analysis Based on a Discretionary-Mandatory Classification”, *International Journal of Information Management,* 28*,* pp. 181-193.

Kahneman, D. & Klein, G. (2009) ” Conditions for Intuitive Expertise: A Failure to Disagree”, *American Psychologist,* 64, pp. 515-526.

Kim, H. & Feamster, N. (2013), ”Improving Network Management with Software Defined Networking”, *IEEE Communications Magazine*, 51, pp. 114-119.

Klinkerman, S. (1996), “Survey finds radical transformation” *Bank Management,* 72, pp. 30-31.

Limnéll, J., Majewski, K. & Salminen, M. (2014), ”Kyberturvallisuus”, *Docendo Oy, Jyväskylä.*

McCall, G. & Simmons, J. (1969), “Issues in Participant Observation: A Text and Reader”, *Addison-Wesley, Reading, Mass.*

McKinnon, J. (1998), “Reliability and Validity in Field Research: Some Strategies and Tactics”, *School of Economic and Financial Studies, Macquarie University.*

Olin, P., Koivuniemi, M., Lehto, M., Luukkainen, K., Magd, N., Nevaste, N., Niinikorpi, S., Rautio, J., Ristolainen, M., Sjöroos, M., Tuovinen, J., Kouki, P. & Suhonen, S. (2018), ” Kyberturvallisuuden sanasto”, *Sanastokeskus TSK,* Helsinki.

Power, R. (2000), “Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare”, *San Francisco, CA: Computer Security Institute.*

Prawitt, P., Smith, J. & Wood, D. (2009), “Internal audit quality and earnings management”, *Accounting Review,* Vol. 84, Issue 4, pp. 1255-1280.

Rustagi, S., King, W., & Kirsch, L. (2008), “Predictors of Formal Control Usage in IT Outsourcing Partnerships”, *Information Systems Research*, 19, pp. 126-143.

Scapens, R. (1990), “Researching management accounting practice the role of case study methods”, *British Accounting Review,* 22, pp. 259-281.

Schwartz, M. & Schwartz, C. (1955), ”Problems in Participation Observation”, *American Journal of Sociology*, pp. 343-354.

Simon, J. & Burstein, P. (1985), “Basic Research Methods in the Social Sciences”, 3rd edition, *Random House, New York.*

Siurdyban, A. (2014), ”Understanding the IT/business partnership: A Business Process Perspective”, *Information Systems Frontiers*, 16, pp. 909-922.

Thevenin, S. (1997), “Teaching an old audit new tricks”, *The Internal Auditor*, 54, pp. 58-65.

Ward, J., Daniel, E. & Peppard, J. (2008), “Building Better Business Cases for IT Investments”, *MIS Quarterly Executive Vol. 7 No. 1 / Mar 2008 1.*

Yin, R. (1984), “Case Study Research, Design and Methods”, *Sage Publications, Beverly Hills.*

8 Muut lähteet

Centre for the Protection of National Infrastructure (CPNI, 2009), “Risk Assessment for Personnel Security - A guide”, 3rd Edition, United Kingdom.

Computer Security Institute (CSI, 2002), "Computer Security Issues and Trends: 2002 CSI/FBI Computer Crime and Security Survey" http://www.gosci.com.

Dietrich, G., Goles, T. & White, G. (2004), “Cyber Security Exercises: Testing an Organization’s Ability to Prevent, Detect, and Respond to Cyber Security Events”, Proceedings of the 37th Hawaii International Conference on System Sciences.

Vilander, H. (2019), “Whitepaper: Cybersecurity Exercises Expose Vulnerabilities in Decision-Making”, Nixu Oyj. URL: “https://www.nixu.com/whitepaper/whitepaper-cybersecurity-exercises-expose-vulnerabilities-decision-making”.

IIA Position Paper (2013): “The Three Lines of Defence in Effective Risk Management and Control”.

ISACA (2018): “Cobit 2019 Framework – Intorduction and Methodology”.

ISO/IEC 27001: 2005, Information technology - Security techniques - Information security management systems - Requirements (2005).

National Industrial Defense Association (NDIA) (2000), "Computer Network Defense: An Industry Perspective," an NDL\ Study in support of U.S. Space Command, unclassified.

9 Liite 1: Tietoturvaa kotona ja työpaikalla

Rousku, K. (2014), ”Kyberturvaopas – Tietoturvaa kotona ja työpaikalla”, *Talentum.*

Työpaikalla muistettavaa

	Noudatettava asia	**Perustelut**
Ulkoisten uhkien torjuminen	Pidä kuvallinen henkilökortti aina näkyvillä.	Henkilökortti varmistaa, että oikeat ihmiset saavat liikkua organisaation tiloissa.
	Ohjaa kuvakortittomat ulos tai vastaanottoon.	Ulkopuolisen on helppo soluttautua postinkantajaksi tai muiden tuotteiden toimittajiksi.
	Näyttöjen suojakalvojen käyttö. Näyttöjen lukitseminen aina kun poistutaan työpisteeltä.	Työntekijän tulisi tiedostaa, millä tavalla omia tietojaan luokitellaan, ja pyrkiä estämään ulkopuolisten urkintayritykset. Myös organisaation sisällä.
Tietojen säilyttäminen	Säilytä kaikki muu paitsi julkinen tieto lukituissa tiloissa. Tietokoneiden lukkiutuminen. Kannettavien tietokoneiden kiintolevyt tulisi salakirjoittaa.	Työntekijöiden tulisi tiedostaa, miten hänen tiedostonsa luokitellaan (erittäin salainen-julkinen-asteikolla). Salassa pidettävien tietojen säilyttämistä ohjaavat kansainväliset lait ja asetukset.
Tietojen käsittely	Työntekijöiden tulisi tiedostaa tietojen luokittelu. Esim. osoite- tai läsnäolotiedot.	Tietoja käsitellään helposti liian tiukasti tai liian varomattomasti. Kaikki tieto tulisi pystyä luokitella esim. neljäportaisen asteikon mukaan.
	Kun tietoja jaetaan muiden käyttäjien kanssa, jakajan tulisi varmistua vastaanottajan tietoluokituksesta.	Vastaanottajalla tulee olla oikeus kyseiseen tietoon.
	Huolehdi, että tieto on varmuuskopioitu ja että sama tieto on saatavilla useammasta paikasta (työpaikan verkkolevy & paikallinen kovalevy). Tietojen synkronointi.	Näin huolehditaan siitä, ettei tietoa pääse häviämään. Eheys & saatavuus.
	Tiedosta, että työstetyn tiedoston väliversioita voidaan tarvita. Tallenna ja erota väliversioita juoksevalla numeroinnilla.	Samalla nimellä tallentaessa tietoja voi hävitä vuosien saatossa.
Tietojen lähettäminen ulkopuoliselle taholle	Tiedosta tiedon salausluokka. Salakirjoita sähköpostit ja muodosta salattu yhteys tarvittaessa. Kuriiripalvelua voidaan käyttää isompien tiedostojen lähettämiseen: huolehdi kuriiripalvelua tarjoavan organisaation käyttämästä suojauksesta.	Tiedon lähettäminen tietoverkkoa pitkin aiheuttaa monenlaisia uhkia: yhtiöiden välinen viestiminen voi aiheuttaa epäilyksiä, tietoa voidaan muokata lähetyksen aikana jonkun ulkopuolisen toimesta → varmista tietyntasoinen salaus.
Tietojen turvallinen hävittäminen	Varmista tietojen oikeanlainen poistaminen. Fyysinen tuhoaminen ja tiedostojen tuhoaminen.	Tietoja voidaan kaivaa kovalevyiltä vaikka ne olisivat kokonaan poistettuja.

Pöytätietokoneen kanssa muistettavaa

Haittaohjelmien estäminen	Älä asenna sellaisia ohjelmia koneelle, joiden asentamiseen ei ole annettua lupaa.	Useat netistä hankitut ohjelmat eivät vaadi ylläpitäjän oikeuksia. Samalla ne kuitenkin saattavat sisältää haitallisia ohjelmia, jotka voivat esimerkiksi seurata käyttäjän toimia ja lähettää ne eteenpäin.
Admin-käyttäjä	Käytä tätä oikeutta vain silloin, kun sille on erillinen tarve. Muuten käytä alemman tason peruskäyttäjää.	Näin voidaan estää tahattomien ohjelmien ja muiden käyttöoikeuksien väärinkäyttö.
Ohjelmapäivitykset	Aseta automaattiset käyttöjärjestelmäpäivitykset päälle.	Päivitysten yhteydessä yleensä paikataan jotain tietoturva-aukkoa, ja lisätään ohjelmiin uusia toimintoja.
Salasanojen käyttö	Käytä eri salasanoja eri palveluissa.	Yhden palvelun tietomurto voisi johtaa muiden palveluiden tietojen kalasteluun.
Mikrofoni ja kamera	Peitä mikrofoni ja kamera silloin kun niitä ei käytetä.	Kameraa ja mikrofonia voidaan käyttää tietämättäsi esimerkiksi jonkun haittaohjelman toimesta.

Kannettavan tietokoneen kanssa muistettavaa

VPN:n käyttö	Salaa verkkoyhteytesi joko VPN:llä tai käytä salasanalla varustettua reititintä.	Verkkotoimintaa voi kuunnella, jos käyttäjä ei salaa yhteyttään. Esimerkiksi käyttäjätunnuksia voi vuotaa väärien ihmisten käsiin salaamattoman yhteyden käytöstä.
Etäyhteyden luominen	Käytä kryptattua SSH-etäyhteyttä, jos sinun tulee päästä käsiksi työpaikalla oleviin tiedostoihin.	Samasta syystä kuin edellä.
Päätelaitteen hukkuminen (yleisesti)	Älä missään olosuhteessa jätä laitettasi ilman valvontaa.	Muista salakirjoittaa tärkeät tiedostot ja ottaa näistä varmuuskopiot työpaikan omalle palvelimelle sekä ulkoiselle kovalevylle.

Älypuhelimen kanssa muistettavaa

Päätelaitteen etälukitseminen ja tietojen poistaminen	Jos älylaite hukkuu, pyri mahdollisimman nopeasti tekemään laitteen lukitseminen ja tietojen poistaminen.	Nykyään puhelinvalmistajat mahdollistavat pilven kautta tehtävän etälukituksen ja tehdasasetuksien palauttamisen. Näytä käyttämällä voidaan vaikeuttaa ulkopuolisen tekemää haittaa.
Sovellusten pyytämien toimintojen salliminen	Älä salli mitään sovelluksien pyytämiä toimintoja ellei organisaatiolla ole tähän jotain muuta ohjetta.	Monet sovellukset pyytävät aivan turhia tietoja puhelimen toisilta sovelluksilta, esim. osoitekirja.

Yleistä muistettavaa

Sähköisten tietojen turvallinen kuljettaminen	USB-tikut.	Varmistu USB-tikkujen ja muiden ulkoisten muistien salaamisesta.
www-sivut & selain	Varmistu domainista. Varmista, että yhteys nettisivuun luodaan turvallisen protokollan avulla (HTTPS). Älä lataa selaimen lisäohjelmia tai -toimintoja.	Nämä vaarantavat käyttäjän turvallisuuden. Selaimen lisäohjelmat voivat muuttaa käyttäjän toimintaa.

10 Liite 2: Haastattelukysymykset tutkielmaan ”Yritysjohdon vastuu/tilivelvollisuus yrityksen kyberturvakysymyksissä.”

KRIITTINEN INFRASTRUKTUURI

Kriittisen infrastruktuurin yhteiset kehityshankkeet: keskitetysti johdetut hankkeet tuovat kustannushyötyjä.

- **Mikä on kriittistä infrastruktuuria?**
- **Kriittisen infran luokittelu yhtiössä?**
- **Onko yhtiöllä yhteishankkeita tietoliikenneratkaisujen kehittämisessä? Jos on, millaisia nämä ovat? Kuvaile.**
- **Asettaako regulaatio rajoitteita tietoliikenneratkaisujen kehittämisessä?**

ORGANISAATIO

Organisaatiorakennne: miten organisaatio on rakentunut?

- **Miten organisaation vastuunjako ja päätöksenteko on toteutettu?**
- **Päätöksenteko voidaan hoitaa joko keskitetysti tai sitten hajautetusti IT-asioiden suhteen. Miten teillä on?**
- **Miten kuvailisit tietoturvahankintojen prosessia?**
- **Miten meneillään olevaan IT-hankkeeseen hyväksytään lisätöitä?**
- **Miten tietoturva varmistetaan järjestelmähankkeissa?**
- **Varahenkilöjärjestelyt?**
- **Voisitko kuvailla, miten toimintatapojen yhtenäisyys varmistetaan?**
- **Onko organisaatio matriisi- vai hierarkkinen kokonaisuus?**
    - **Miten rajapinnoissa tapahtuva turvallinen tietojen siirtoa/vaihto liiketoimintayksiköiden välillä varmistetaan?**
- **Miten tietoturvasta raportoidaan johdolle?**
- **Onko tietoturva eriytetty muusta IT-yksiköstä?**
- **Onko organisaatiolla ulkoistettuja liiketoimintoja?**
    - **Miten tietoturva on otettu huomioon ulkoistuksissa?**

Kilpailuympäristön vaikutukset: organisaation aineettoman omaisuuden arvo, sektorin muutoksen tila, alalle tulon esteet, organisaation oma positio markkinalla.

- **Miten suuri osuus taseesta on aineetonta omaisuutta ja mistä eristä se koostuu? Entä taseen ulkopuolinen aineeton arvo?**
- **Miten näette aineettoman omaisuuden yhtiön menestykseen pitkällä aikavälillä?**
- **Voisiko jokin sidosryhmä hyötyä organisaation aineettomasta omaisuudesta?**
- **Millaisia muutoksia sektori kohtaa tällä hetkellä? Kuvaile näitä.**
- **Miten vaikeaa tälle alalle on päästä? Sisältyykö siihen jotain erikoisia vaatimuksia?**
- **Onko yhtiö vakiinnuttanut oman position markkinalla? Miksi/miksi ei?**
- **Mikä on suhteenne mediaan nyt ja miten se mahdollisesti kehittyy tulevaisuudessa?**

Organisaatiokulttuuri: millaisia uskomuksia, rituaaleja tarinoita organisaatiolla on? Mitä erityislaatuisia tapoja organisaatiolla on, joita ei välttämättä ole muilla?

- **Millaisissa eri tilanteissa eri tahojen identiteetin varmentaminen on tärkeää? Miten näiden tahojen henkilöllisyys varmennetaan?**
- **Yhtiön sisäisen tyytyväisyyden mittaaminen: miten työntekijöiden tyytyväisyyttä mitataan?**

Liiketoimintojen standardointi: miten paljon henkilöstö hoitaa tehtäviään ennalta sovittujen kriteereiden mukaisesti? Entä, miten paljon työtehtäviin liittyy soveltamista ja näkemyksen ottoa? Miten soveltavissa työtehtävissä on otettu huomioon tehtävään käytetyt valtuudet?

- **Miten tietoturva liittyy työtehtävien standardointiin?**
- **Miten kriittisiä työtehtäviä valvotaan/seurataan tietojärjestelmän avulla? Kuvaile näitä.**
- **Otetaanko työtehtävien suunnittelussa huomioon mahdolliset vaaralliset työyhdistelmät? Miten nämä otetaan huomioon riskienhallinnassa?**

Koulutus ja tietoisuuden lisääminen: millainen koulutuksen kulttuuri organisaatiossa vallitsee tietoturva-asioiden suhteen?

- **Järjestetäänkö tietoturvaharjoituksia/-koulutuksia jatkuvasti? Miten usein? Pidetäänkö henkilöstö jatkuvasti ajan tasalla mahdollisista uhista, jotka voivat liittyä järjestelmiin, sovelluksiin tai laitteistoon? Miten näistä puhutaan?**

TEKNOLOGIA

Palomuurit ja tunkeutumisen havaitseminen: miten nämä turvaavat organisaation omaisuuden ja tiedot?

- **Millainen tietoturvan hallintajärjestelmä yhtiöllä on?**
- **Onko ulkoapäin tuleville uhille tehty riskikartoitusta, ja jos on, millaista?**
- **Miten uhista puhutaan organisaatiossa?**
- **Onko yhtiön ulkoverkkoon ja sisäverkkoon tehty tekninen tietoturvatarkastus? Jos on, niin minkälainen?**
- **Valvooko järjestelmät aktiivisesti verkkoliikennettä?**

Monitasoisten salasanojen käyttö: tiedon lukemiseen ja muokkaamiseen voidaan vaatia monta tunnustautumistapaa.

- **Luokitellaanko yhtiön tietoja eri tasoisiksi julkinen-salainen-asteikolla?**
- **Käytetäänkö monitasoisia salasanoja organisaatiossa esimerkiksi salaisiin tietoihin pääsemiseksi?**
- **Käytetäänkö 2-vaiheista tunnistautumista yhtiön sisällä?**

Julkisen avaimen infrastruktuuri

- **Miten yhtiön tiedostoja salataan?**
- **Suojataanko yhtiön läppäreiden kovalevyjä?**

Palvelinten turvallisuus

- **Miten palvelinten turvallisuus varmennetaan?**
- **Palvelinten segmentointi?**

YLIN JOHTO

Kriittisen tiedon ja järjestelmien tunnistaminen

- **Luokitteleeko yhtiö tietoaan, ja jos luokittelee, niin miten se sen luokittelee?**
- **Miten ylin johto huolehtii tietojen luottamuksellisuudesta?**
- **Miten ylin johto huolehtii tietojen eheydestä?**
- **Miten ylin johto huolehtii tietojen saatavuudesta?**

- **Miten ylin johto huolehtii toimintojen jatkuvuudesta?**

Riskien arviointi: millä tavoin erilaisiin väärinkäytöstilanteisiin on varauduttu? Onko näille tehty riskiarviota? Onko eettinen yhteydenottokanava (whistleblowing)?

- **Onko toipumissuunnitelmaa?**

Kontrollien asettaminen

- **Miten ylin johto arvioi nykyisten kontrollien toimivuutta?**
- **Miten ylin johto asettaa kontrolleja?**

11 Liite 3: Tutkimuksessa haastatellut organisaatiot

Haastattelukysymyksien laatiminen toteutettiin yhdessä

IA Insight Oy

Haastatellut asiantuntijaorganisaatiot

Akselera Finland Oy

Asianajotoimisto Krogerus Oy

IA Insight Oy

Kreate Oy

PricewaterhouseCoopers Oy

Rettig ICC Oy Ab